Quantum communication and security

Mu Yi

University of Wollongong

Recommended Citation
Quantum Communication and Security

A thesis submitted in fulfilment of the requirements for the award of the degree of

Master of Science (Honours)

from

UNIVERSITY OF WOLLONGONG

by

Yi Mu, Ph D (1994)

Department of Computer Science
1994
This dissertation is composed of the results of our investigation in quantum cryptography - a new topic in computer security. The goal of this study is to explore useful schemes for quantum cryptographic communications.

The focus of our study is an investigation into quantum cryptographic protocols based on quantum-mechanical uncertainty principle and Bell’s inequality. First, we use the theory of quadrature phase amplitudes and quantum homodyne detection to establish a new quantum key distribution protocol which relies on an optical coupler. In this work we propose, for the first time, the use of this theory in quantum cryptography. Second, we investigate Ekert’s protocol using Bell’s theorem. The contents in this investigation is not new, but we use our calculation to prove that Ekert’s protocol is true for both photon-based and spin-$\frac{1}{2}$-particle-based systems. Third, we study a quantum coherence key distribution constructed using Bennett and Brassard’s protocol. The information theory of the system is used to study the scenario where eavesdropping occurs. Finally, we explore the theory of quantum nondemolition detection (QND) to investigate the results when eavesdropping occurs. A calculation for the QND, using parametric frequency conversion, is given for two different quantum cryptographic systems.

Our study is undertaken with the aid of some knowledge of physics, therefore, before our main results are presented, we introduce some useful physics which may help readers understand the contents of our work.
The publications resulted from this work include: (1) "Shared cryptographic bits via quantized quadrature phase amplitudes of light" (Optics Communications, Jan., 1996), and (2) "Multi-user quantum cryptography", in Proceeding of International Symposium on Information Theory & Its Applications, Sydney, 1994.
## CONTENTS

| ACKNOWLEDGEMENTS                  | ii |
| ABSTRACT                          | iii |
| 1 INTRODUCTION                    | 1 |
| 1.1 Historical review of quantum cryptography | 2 |
| 1.2 Topics studied in this thesis  | 7 |
| 2 CRYPTOGRAPHICALLY USEFUL FUNDAMENTAL QUANTUM PRINCIPLES | 11 |
| 2.1 Establishment of quantum physics | 11 |
| 2.2 Wave and particle property     | 14 |
| 2.3 Heisenberg's uncertainty principle | 15 |
| 2.4 The uncertainty principle against eavesdropping | 18 |
| 2.5 Entangled states              | 20 |
| 2.6 EPR nonlocal realism          | 22 |
| 2.7 Bell's theorem                | 25 |
| 3 CRYPTOGRAPHIC PROTOCOLS BASED ON THE UNCERTAINTY PRINCIPLE | 29 |
| 3.1 BB protocol                   | 29 |
| 3.2 Quantum cryptography using four nonorthogonal states | 33 |
### 3.3 Conclusion  

<table>
<thead>
<tr>
<th>4 QUANTUM CRYPTOGRAPHY BASED ON BELL'S INEQUALITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1 Introduction</td>
</tr>
<tr>
<td>4.2 Photon-Based System</td>
</tr>
<tr>
<td>4.3 Spin-$\frac{1}{2}$-particle-Based System</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5 QUANTUM CONFERENCE KEY DISTRIBUTION SYSTEMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1 Conference Key Distribution Protocols</td>
</tr>
<tr>
<td>5.2 Information Theory of MultiUser Cryptosystems</td>
</tr>
<tr>
<td>5.3 Correlations in Quantum Cryptosystems</td>
</tr>
<tr>
<td>5.4 Discussion and Conclusion</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6 EAVESDROPPING BY QUANTUM NONDEMOLITION DETECTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1 Bennett's two-state system and eavesdropping by quantum non-demolition detection</td>
</tr>
<tr>
<td>6.2 The QND attack on the protocol using an optical coupler</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>7 CONCLUSION</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>REFERENCES</th>
</tr>
</thead>
</table>


INTRODUCTION

In conventional cryptography and information theory it is taken for granted that digital communications can always be passively monitored, and that an eavesdropper learns the entire contents of a communication, without the sender or receiver being aware that any eavesdropping has taken place. Quantum cryptography enables two people to exchange messages with perfect security unattainable by conventional cryptography. The central idea behind quantum cryptography is that an eavesdropper cannot monitor transmission without being noticed by the participants.

Since quantum cryptography was invented 15 years ago, approximate 80 research papers have been published in journals and conference proceedings worldwide. This research has yielded some interesting protocols, mainly based on Heisenberg's uncertainty principle and quantum correlation. Our study is devoted to some interesting quantum cryptographic protocols in optical communications.

The aim of this chapter is to review previous studies in quantum cryptography and to introduce our work.
1.1 HISTORICAL REVIEW OF QUANTUM CRYPTOGRAPHY

Quantum cryptography was born in the late 1960s when Stephen Wiesner wrote "Conjugate Coding" [1]. Unfortunately, his paper was not published. Charles H. Bennett and Gilles Brassard were the first people to recognize the importance of Wiesner's idea and brought quantum cryptography to life. The first paper on quantum cryptography, written by C.H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner, was published in 1983.[2] Subsequently, Wiesner's original paper was published in *Sigact News* [1]. At present, about 80 relevant papers have been published. A valuable summary of these papers (up to 1993) is given in the bibliography by Brassard [3].

Exploitation of quantum effects in cryptographic communications can yield significant and novel benefits not anticipated by classical physics. Quantum cryptography is based upon quantum mechanical phenomena, such as Heisenberg's uncertainty principle and quantum correlation. The latter is represented by the famous EPR or Einstein-Podolsky-Rosen-Bohm *gedankenexperiment* [4, 5]. A well-known protocol using the uncertainty principle was proposed by Bennett, Brassard and co-workers in [6, 2]. This protocol is now called BB protocol. The BB protocol shows that information can be encoded in one of four nonorthogonal quantum states (based on photon polarization) using two bases in such a way that any attempt to extract the information by an eavesdropper will randomize and hence destroy the information. In other words, the eavesdropper's acts will definitely cause a change in the signal between the legitimate users, therefore revealing the presence of the eavesdropper. On the other hand, it has also been demonstrated that the EPR and Bell's theorem or inequality [7] is useful in quantum cryptography. Protocols based on the EPR and Bell's theorem exploit the properties of quantum-correlated particles. As eavesdropping unavoidably introduces some local condition caused by the measurement, it causes the data
measured by legitimate users to display no violation of Bell's inequality and then reveals the attempt of interception [8]. A further simplified protocol which does not use Bell's inequality has been proposed by Bennett, Brassard, and Mermin [9]. Although there are some other interesting protocols, for instance, based on photon interferometry [10], teleporting [11], rejected-data [12], and so on, the BB protocol and Ekert's protocol [13] are the most important models in quantum cryptography.

The BB protocol employs Wiesner's original idea using the Heisenberg's uncertainty principle. Detailed references for this protocol can be obtained from Ref.[6, 2, 1, 14, 15]. We will also give more details about the BB protocol in next chapter. Here we only briefly introduce this protocol. The BB protocol is constructed using four polarized photon states which belong to two bases, basis-one and basis-two, with two states for each basis. The measuring operator based on basis-one can precisely measure the states in basis-one only; if we use it to measure the states in basis-two, the outcome will be totally random, and vice versa for the measuring operator based on basis-two. In the BB protocol, a sender (say Alice) sends a sequence of polarized single photons, which are randomly chosen from the four polarized photon states, to a receiver (say Bob) who randomly and independently chooses a measuring basis to measure each photon. After completing all the measurements, Bob announces publicly which basis has been used for each photon (but not the results of the measurements). Alice and Bob discard the results in which Bob failed to detect a photon and those for which the measurements were made using a polarization basis different from the one used by Alice. The remaining results are checked by comparing a large subset of these remaining results. If they agree, the remaining results not yet revealed can be used as a key, so achieving a quantum key distribution. If an eavesdropper (say Eve) tries to read the quantum channel, she will not be able to measure the signal correctly due to the lack of basis information. Hence, Eve, attempting to use the
intercept/resend, cannot reconstruct the signal sent by Alice, if she wants to use
the way of intercept/resend. This is because her measurement (if she randomly
chooses the measuring basis) yields random results only. If she resends all pho-
tons generated using the result of her measurements, it will still cause substantial
errors in the measurements made by Bob. Although Alice will announce publicly
which basis is correct for each of Bob’s measurement after the communication
has been completed, it is too late for Eve since each of her measurements had
been carried out before Bob’s measurement was performed.

The BB protocol relies on the two non-commuting bases. Using states in only
one of the bases, we are unable to obtain any useful protocol via the BB-type
idea. Using a totally different idea, Ekert [13] proposed a new type of quantum
cryptographic system which could be built by modifying the apparatus that Alain
Aspect and coworkers [5, 16] used to test Bell’s inequality. In Ekert’s system, a
source placed between Alice and Bob emitting spin-$\frac{1}{2}$ particles in a singlet state.
These particles are basically correlated electron pairs (or they can use a two-
photon state as an alternative). One particle in the singlet state is sent to Alice
and the other to Bob. Alice and Bob set their analyzers to an orientation which
is randomly and independently chosen from one of the specified orientations, for
instance, horizontal, vertical, or diagonal, and measures the spin of incoming par-
ticle. After the whole signal string has been transmitted, Alice and Bob announce
publicly which orientation was used for each singlet state. Using Bell’s theorem,
consequently, Ekert can guarantee the security of those instances measured when
both Alice and Bob use the same orientation, these instance can thus be used as
a secret key.

It seems that Ekert’s system is automatically secure, since the particles contains
no information until the measurements are performed by Alice and Bob. However
Eve might try to circumvent the system by substituting her own choice of particle
states in place of those from Alice and Bob’s source. However this will fail because she does not know the orientations that Alice and Bob will choose for their analyzers. Her intervention would be equivalent to the introduction of elements of physical reality or local condition, thus the correlation function will not have the correct quantum-mechanical value.

Ekert arranged his data analysis in such a way that Alice and Bob partition the outcome of the measurements into two groups: group-one contains the instances where they have both used the same orientation; group-two contains those where they have used different orientations. Using group-two, Alice and Bob calculate the correlation of the measurements. If they find the outcome of the calculation agrees with Bell’s inequality, they can assume that there must be some sort of eavesdropping that happened during their communication. Otherwise, if the outcome violates Bell’s inequality, the correlation must be prefect and the instances in group-one are usable by them as a secret key.

Bennett et al. [9] suggested that the EPR-type system can be constructed without using Bell’s inequality. Their scheme is basically equivalent to their original protocol which requires the uncertainty principle.

Bennett [10] also proposed a system using only two quantum states, instead of the four in the previous model. Alice can start the key distribution protocol by sending Bob a sequence of binary states, based on two nonorthogonal quantum states, to denote 0 and 1 respectively. Bob has two filters that select states orthogonal to the state corresponding to 0 and the state corresponding to 1 respectively (we define them as filter-0 and filter-1). Filter-0 annihilates state 1, but yields a positive result for state 0, and vice versa for filter-1. After the quantum transmission, Bob tells Alice publicly which measurement had a positive result, but does not say which filter was used. Alice and Bob then discard all instances that do not show a positive result and keep those which are perfectly
correlated as a secret key. Eve does not know in advance which choice Alice and Bob have made in the transmission, so if she could make an apparatus similar to Bob's, she still would not be able to use the appropriate filter. This will make her measurements induce substantial errors into the signal, and thus reveals her attempt at eavesdropping.

Barnett and Phoenix have proposed a quantum cryptographic protocol using three quantum states [12, 17], called it rejected-data protocols. The key point in this protocol is that the analysis of the data obtained, when Alice and Bob used different orientation in their analyzers, can provide useful information regarding whether or not any eavesdropping has occurred. The protocol is somewhat analogous to the Ekert's protocol using Bell's theorem. Hence they were able to construct Bell-type correlation using the three photon states and demonstrated a connection between their result and the protocol using the Bell inequality.

As we noted, security in a quantum cryptographic system is based on the quantum-mechanical principles, such as the uncertainty principle and Bell's theorem. All known quantum cryptographic systems are based on single-particle states, such as a single photon state or a single electron state. In practice, one uses very dim light with intensity less than one on the average (i.e., for instance, sometimes receive zero photon and sometimes receive one photon). Otherwise quantum cryptographic systems would encounter a beam-splitting attack. Fortunately, current photoelectric technology is adequate for making a single-photon state and transmitting it to a distant destination (such as 30 km [18]).

However, a recent development in quantum optics provides us with a light measurement scheme, which presents a promise for measuring a light signal without damaging the signal. This scheme is quantum nondemolition detection (QND). In QND measurement the signal is not physically measured, instead, a probe
mode which is interacted with the signal mode is measured by a detector. After interaction, the probe light may contain full information of the signal.

Is it bad news for quantum cryptography? We hope not. Werner and Milburn [19] have obtained a negative result, when they used a method involving photon-number QND measurements to eavesdrop a Bell-type system. They showed that eavesdropping causes a violation of quantum-mechanical principle under a QND measurement. We will, in this thesis, give some detailed studies about the QND which will be introduced in later part of this chapter.

A great interest in experimental realization of quantum cryptographic communication has recently been seen. Experiments carried out include those for the BB protocol [6, 20], the EPR-type system [8], and single photon interference[21]. The first experimental demonstration of the BB protocol was done by Bennett et al. [6], in their experiment, using a hashing technique, a very low error rate was achieved. In the latest experiment, Muller and coworkers [20] have also successfully demonstrated the BB protocol. They were able to use an optical fibre over more than 1 km and achieved a very low error rate. Also, according to a recent paper [18], Marand and Townsend have achieved quantum key transmission using a 30 km long optical fibre interferometer.

1.2 TOPICS STUDIED IN THIS THESIS

Our attempt in this thesis is to investigate quantum cryptographic protocols. Our study extensively involves fundamental physics knowledge, but it should be suited for readers who have a little background knowledge in physics and a good background in cryptography. Our interests are in these particular areas: protocols using quadrature phase amplitudes of a light field, protocols based on Bell-type inequalities (is basically Ekert's protocol, but via our calculation),
protocols for conference key distribution, and quantum nondemolition detection against quantum cryptographic systems.

In the first work, we develop a quantum cryptosystem which allows a cryptographic key bit to be encoded using four nonorthogonal quantum states described by non-commuting quadrature phase amplitudes of a weak optical field (but not photon polarization!). Our system is secure, since the nonorthogonal states are designed to have a large multi-overlap, hence it is impossible to obtain a certain result when performing a measurement on one of these states. The realization of this protocol relies on an ordinary photon-coupling apparatus which allows cryptographic signal to couple with squeezed light. Such coupling scheme provides a secret shared key for the legitimate users involved.

Ekert’s protocol is the first protocol based on Bell’s inequality. In this thesis, we re-study it using both photon-based and spin-$\frac{1}{2}$-particle-based models. Under our calculation, it is shown that Bell’s inequality is satisfied in by both the photon-based and the spin-$\frac{1}{2}$-particle-based systems when eavesdropping takes place. We should state that our calculation result is not new.

Multi-user key distribution is called conference key distribution. A classical conference key protocol was studied by Ingemarsson, Tang, and Wong [22]. However, a quantum channel is different in that it is a closed-single-line channel and so only communication between two users is allowable, while a classical channel can be allowed to extract information by multiusers. An open question is whether we can have a multi-user quantum cryptographic system. In this work, we study conference key distribution protocols based on the BB protocol. The system information theory and correlation are studied for two basic conference key distribution systems: fan-shaped and series configuration. It is however noted that there are some practical problems on the implementation of conference key protocols we have proposed. These problems include security (for one Fan-shaped
configuration) and quantization. Some of problems are fundamental and are unsolvable, whereas we should include the contents which at least demonstrate the flaws.

The security of a quantum cryptographic channel can be undermined by the activities of an eavesdropper who can perform measurements on fields as they travel from the sender to the receiver. Suppose that the possibility of a beam-splitting attack has been eliminated by use of faint particle beams, then Eve’s strategy might turn to using methods which involve more advanced physics, such as the QND technique. Our investigation will focus on the QND schemes using parametric frequency conversion [23]. We will demonstrate that for a private quantum channel, the QND scheme will also be restricted by the uncertainty in the detection process, whereas an encrypted signal may be in principle conserved (but in practice suffers some losses).

The contents of this work are organized as follows, In Chapter 2 we review some fundamental physical concepts which are useful for quantum cryptography. We mainly address the questions, such as, “What is quantum physics?” “What are the properties of particle-wave?” “What is the uncertainty principle?” “What are the EPR paradox and Bell’s theorem?” etc.. This information will help readers to understand quantum cryptography and our work.

Chapter 3 is devoted to protocols based on uncertainty principle. The main purpose in this chapter is to investigate one novel protocol using quadrature phase amplitudes of light, especially, where an optical coupler is employed to realize the protocol. The BB protocol will also be introduced to enable comparison before proceeding to the investigation of our protocols. Part of the contents in this section has been published in Optics Communication [24].

In Chapter 4, we study Ekert’s protocol based on Bell’s theorem.
Chapter 5 studies the protocols of quantum cryptographic conference key distribution and the information theory of a system where eavesdropping has occurred. Our goal is to investigate how the BB protocol will perform if multi-users require a common key distribution. Part of the contents in this chapter has been published in the Conference Proceeding of ISIT (1994). [25]

In Chapter 6, we investigate an eavesdropping strategy based on the QND measurement. Bennett's system [10] and our system studied in Chapter 3 will be investigated.

Chapter 7 is the conclusion.
Quantum theory is the basic theory which precisely describes microscopic physics. It is generally realized that quantum theory represents a radical change, not only in the content of scientific knowledge, but also to the fundamental concepts in the terms with which such knowledge can be expressed. Nowadays, quantum theory has been extensively applied in science. One surprising application of quantum theory is in the field of secure communications. The fundamental theories which guarantee the security are the uncertainty principle of quantum mechanics and correlations of quantized particles. The purpose of this chapter is to introduce some important quantum concepts which are directly relevant to quantum cryptography.

2.1 ESTABLISHMENT OF QUANTUM PHYSICS

To understand the basic principles of quantum mechanics, we need some historical background knowledge of quantum mechanics. In the 17th century Newton and several other great scientists developed a successful theory to explain motion of objects. This theory is called classical mechanics. Newton's explanation of motion in terms of forces, momentum and acceleration is encapsulated in his three laws of motion, which successfully describe the motion of macroscopic bodies, such as cars, planets etc.. Perhaps the most successful application of Newton's
theory is the exploration of space. Generally, nowadays, the usefulness of classical mechanics for sending a space shuttle to the moon is assumed.

In the period of the late of the 19th century and the beginning of 20th century, Newton's classical mechanics was generally regarded as having been completely developed, however it also encountered serious problems, particularly at the very small distance involved in the study of atoms and molecules.

Historically, quantum theory began with the attempt to interpret the equilibrium distribution of electromagnetic radiation from a blackbody. In the 1800's, rapid developments in the metallurgy of high temperatures pushed forward the study of heat radiation. In the late 19th century, it was realized that heat radiation is a kind of electromagnetic radiation. This gave the impetus to intensive studies in electromagnetic radiation in both theory and experiment, especially for blackbody radiation. Difficulties using classical mechanics were encountered due to the disagreement between the experiment results and predictions of classical mechanics. In Fig. 2.1, the spectral distribution of the energy density as a function of frequency is plotted as evidence of the disagreement. For low frequencies, the spectrum actually does agree with classical physics, but for high frequencies, classical physics predicts a monotonic increase in the energy density, whereas the energy density distribution decreases toward zero.

A physicist, Planck, was able to make a clever guess at an empirical formula representing the energy distribution spectrum, but he was unable to provide a theoretical derivation of the formula with the context of classical physics. Later he found that his empirical formula could be derived by use of a hypothesis of quantization of energy. He adopted a simple model for the walls of the cavity. The walls consist of a large number of electrically charged harmonic oscillators of all possible frequencies. The oscillators exchange energy with the radiation in the cavity. He stated that for a frequency $\nu$ of an electromagnetic radiation, any
substance absorbs and emits it by a unit of $h\nu$, where $h$ is a universal constant of proportionality, later called Planck's constant. In the other words, an absorption or emission must be performed by way of quantization. Planck postulated that the energy of an oscillator of frequency $\nu$ could only be

$$E = n\hbar\nu \quad n = 0, 1, 2, 3, \ldots$$

(2.1)

Although Planck treated the wall as quantized oscillators, he treated the field in the cavity as completely smooth and continuous, as in the classical electromagnetic theory.

Einstein is the first person who quantized electromagnetic fields and predicted that the quantization of energy hypothesis could solve other problems of classical physics. The most famous application is photoelectric effect. Measurements showed that when light strikes the surface of a metal, electrons, or photoelectrons are ejected, depending on the frequency, but not the intensity of light. This contradicts classical electromagnetic theory, which predicted that the energy available in the light is proportional to the intensity and is independent of its frequency. In 1905, Einstein applied Planck's hypothesis to solve the questions
posed by the photoelectric effect and assumed that the energy of a photon is $h\nu$.
When the frequency (or energy) of a photon that strikes the surface of a metal
is large enough, an electron can be knocked out of the metal. According to Ein-
stein’s theory, ultra-violet photons have more energy than visible-light ones, and
so no matter how much visible light you shine on the metal, none of the photons
have enough energy to emit an electron.

Other important questions of the early of 20th century, such as atomic spectrum,
stability of atom, etc., were solved in rapid succession. Nowadays, there is no
doubt that quantum mechanics can precisely describe the atomic world.

2.2 WAVE AND PARTICLE PROPERTY

In classical mechanics a particle is a pointlike mass. Such a classical particle has
well defined position. The motion of the particle proceeds along a well defined
trajectory. However, quantum particles behave very differently.

We now explain the behaviour of quantized particles. In the famous Young’s
interference experiment using double slits, it was demonstrated that light behaved
as a water wave with respect to interference. It might be inferred that light is more
wave like than particle like. However, photons were later discovered. In the 19th
century physicists found that electrons appeared to follow definite trajectories
in cathode-ray tubes. They therefore concluded that electrons were particles.
However, later, a similar experiment using electrons showed a similar interference
pattern to that of light. This cannot be explained by classical theory. Indeed,
electrons, unlike bullets that are pure particles and can be described using using
classical theory, travel like waves! The discovery of the particle properties of light
and the discovery of interference and diffraction effects of electrons demolished
this tidy distinction between particles and waves.
The early quantum theory ways were sought to supplement classical theory with quantization conditions. In 1920's, physicists finally recognized that it would not work without abandoning classical theory. De Broglie took the first step forward and predicted that electrons and other particles have wave properties. De Broglie postulated that the frequency of the wave associated with a particle is related to the energy of the particle by the same equation as for the light wave associated with a photon:

\[ \nu = \frac{E}{h}. \]  

(2.2)

He then deduced that the wavelength of the wave must be related to the momentum of the particle:

\[ \lambda = \frac{h}{p}. \]  

(2.3)

Thus, for the wave associated with a particle moving in the \( x \) direction, he proposed the harmonic wavefunction:

\[ \psi = \sin 2\pi (\nu t - x/\lambda) = \sin \frac{2\pi}{h} (Et - px). \]  

(2.4)

This theory was not widely accepted until confirmed by later detailed experiments of electron diffraction with thin films of metals.

We must conclude that electrons and photons show wave-like interference in their arrival pattern despite the fact they are particles. In this sense we can say that quantum objects sometimes behave like waves and sometimes behave like particles. We cannot explain the magic of quantum mechanics. All we can do is to describe the way quantum things behave. This description is quantum mechanics.

### 2.3 Heisenberg's Uncertainty Principle

We have seen that quantum mechanics does not allow us to visualize the motion of the quantum particle properly due to the properties of wave-particles. This in
fact implies the uncertainty of quantum measurement. Heisenberg first recognized this properties and predicted that, since the quantum-mechanical particles have wave property, they cannot have sharply defined position and velocity, or position and momentum. In the other words, new quantum laws imply a fundamental limitation to the accuracy of experimental measurement. This is the essence of Heisenberg’s uncertainty principle.

Heisenberg’s uncertainty principle can be written down in a precise mathematical form. We now focus on the position and momentum of a quantum-mechanical particle only. Physicists usually talk about momentum meaning the mass of the particle multiplied by its velocity, rather than about velocity. It is familiar that a car’s speed (hence momentum) can be precisely measured at a certain position on a highway. However the measurement of the position and momentum of a quantum-mechanical particle must obey a limitation given by Heisenberg’s uncertainty inequality

$$\Delta x \Delta p \geq \hbar / 2,$$  \hspace{1cm} (2.5)

where $\hbar = h / 2\pi$, $x$ denotes the position of the particle and $p$ denotes the momentum of the particle. $\Delta x$ and $\Delta p$ represent the uncertainties. Heisenberg’s inequality suggests that it is impossible to measure the quantities $x$ and $p$ as accurately as we would wish. In the other words, it is impossible to make both $\Delta x$ and $\Delta p$ small, since the product of the uncertainties must always be equal to or greater than a constant $\hbar / 2$. Speaking more explicitly, if the position is accurately measured, the momentum will be totally random or uncertain, and vice verse.

Planck’s constant may be obtained from experiments of the photoelectric effect. The value of Planck’s constant $\hbar$ is tiny, approximately $6.62 \times 10^{-34}$ Js. Thus, in terms of Eq. (2.5), we can understand why a car’s position and momentum can be coincidently measured with certainty, since the $\hbar$ on the right-hand side of
Heisenberg's uncertainty principle can be precisely proven by using mathematical tools. In general, Heisenberg's uncertainty principle has the form:

$$\Delta \hat{A} \Delta \hat{B} \geq \frac{|\langle [\hat{A}, \hat{B}] \rangle|}{2},$$

(2.6)

where we have used $\hat{\cdot}$ to label quantum-mechanical operator, the commutation relation $[\hat{A}, \hat{B}] \equiv \hat{A}\hat{B} - \hat{B}\hat{A}$, and $\langle \cdots \rangle$ denoting averaging. For example, $\hat{x}\hat{p} - \hat{p}\hat{x} = i\hbar$, which results in (2.5). Inequality (2.6) suggests that any two non-commuting quantum operators cannot accurately and simultaneously be measured.

Heisenberg illustrated the uncertainty principle with some physical experiments. A typical one is electron diffraction, Fig. 2.2. The experiment consists of a horizontal slit through which an electron beam is injected and travels toward the screen where measurement of the positions of the electrons is performed. If an electron passes through the slit, then its vertical position is known within an uncertainty $\Delta x = a$ (the width of the slit). However, because of its wave
properties, the electron will suffer diffraction at the slit and spreads up and down over a range of angles. Let $\theta$ denote the angular width of the central maximum of the diffraction pattern. The width is given by the formula:

$$a \sin \theta = \lambda. \quad (2.7)$$

The vertical component of the momentum has uncertainty given by

$$\Delta p_x = p \sin \theta = \frac{h}{\lambda} \sin \theta \approx h/a. \quad (2.8)$$

The uncertainty relation in this experimental arrangement then is

$$\Delta \hat{x} \Delta \hat{p}_x = \frac{\hbar}{a} \approx \hbar. \quad (2.9)$$

If we want to measure $x$ more accurately, $a$ must be small. This will cause an increase in the uncertainty of $p_x$.

To illustrate the application of the uncertainty principle to quantum cryptography, we will give another example of photon polarization measurement in the next section.

### 2.4 THE UNCERTAINTY PRINCIPLE AGAINST EAVESDROPPING

One of features of quantum mechanics is the uncertainty in the measurements. Heisenberg's uncertainty principle suggests that for two noncommuting observables, accurately measuring one observable necessarily randomizes the value of the other. Now we explain how this uncertainty can be utilized to implement security communication.

Here we focus on photon polarization. A photon can be polarized into the following orientations: horizontal, vertical, left-circular, right-circular, 45° diagonal,
Figure 2.3 Polarized photons pass through a Wollaston prism set at angle $0^\circ$, and $135^\circ$ diagonal. These orientations belong to three bases: $+$, $\bigcirc$, and $\times$, where

\[
+ \rightarrow \{ \text{horizontal, vertical} \}, \\
\bigcirc \rightarrow \{ \text{left-circular, right-circular} \}, \\
\times \rightarrow \{ 45^\circ \text{diagonal}, 135^\circ \text{diagonal} \}.
\]

Observables in two arbitrary bases out of the three do not commute. This implies that accurately measuring a observable in one basis will randomize the observables in the other basis.

We illustrate this in Fig. 2.3 (after Ref. [26]). The detector is a Wollaston prism whose angle is set at $0^\circ$ corresponding to basis $+$, thus the detector can measure photon polarization at either $0^\circ$ or $90^\circ$ with certainty. If we do not set the photon polarization to $0^\circ$ or $90^\circ$, the result of measurement will be a probabilistic one dependent on the angle, because quantum theory tells us that it is impossible to determine this value with certainty. In the special cases, where we choose the angle of photon polarization to be either $45^\circ$ or $135^\circ$, corresponding to basis $\times$, the measuring result shows that half of the photons show up on the left with the angle of $0^\circ$ and half of them show up on the right with the angle $90^\circ$. We have an analogous situation, if we use photons with circular polarizations to replace those with rectilinear or diagonal polarizations.
The implication of the above analysis is that if we choose photons polarized using two arbitrary bases (out of the three) to implement a communication, we might have bonus of adding the security to the communication. As we have said, this is because any eavesdropping using a wrong basis will randomize the photon polarization, and this can be detected by the receiver. A more detailed analysis will be given in the next chapter.

2.5 ENTANGLED STATES

Since quantum-mechanical particles have the properties of both particles and waves, they have to be described by a wavefunction or a quantum state. A simple example of a wavefunction is given by equation (2.4). The behavior of a wavefunction is determined by the corresponding Schrödinger equation. Here, we do not attempt to go into details of Schrödinger equation but intend to explain entangled wavefunctions which are directly relevant to the subject of this work.

How is a quantum measurement performed? Suppose that there is a quantum-mechanical measuring operator, $\hat{H}$, which measures a quantum state $\psi_1$ (one of the eigenstates of $\hat{H}$). In the simplest case, we have,

$$\hat{H} \psi_1 = E_1 \psi_1, \quad (2.10)$$

where $E_1$ is the only eigenvalue of the measurement. If $\hat{H}$ is used to measure the other state $\psi_2$ we obtain the sole eigenvalue $E_2$,

$$\hat{H} \psi_2 = E_2 \psi_2. \quad (2.11)$$

$\psi_1$ and $\psi_2$ can be used to construct a superposition state

$$\Psi = c_1 \psi_1 + c_2 \psi_2. \quad (2.12)$$
Figure 2.4 The arrangement of the beamsplitter which produces entangled states.

The measurement of $\Psi$ using $\hat{H}$ becomes uncertain and can be only described by probabilities. It can merely be predicted that there is a $|c_1|^2$ of probability of obtaining $E_1$ and a $|c_2|^2$ probability obtaining $E_2$, where $|c_1|^2 + |c_2|^2 = 1$.

A physical system may consist of several quantum objects, for example, the outer orbit of oxygen consists of two electrons, which can be described by a singlet quantum state - a kind of entangled state. An entangled state cannot be decomposed into a product of two states. For example, if $\Psi(x_1, x_2)$ is an entangled state, there is no way to write it into the form of $\Psi(x_1, x_2) = \Phi(x_1)\Phi(x_2)$. The state of an oxygen atom may be considered as an entangled state of the electrons.

We focus only on Schmidt-type entangled states (or Schmidt decomposition), which are directly relevant to our topic. Suppose now that there are two initial states of photons, $|\alpha\rangle$ and $|\beta\rangle$, which are coupled through a beamsplitter arranged as shown in Fig. (2.4). The entangled state for beam 1 and 2 is written as:

$$|\Psi\rangle = c_1|\alpha\rangle_1|\beta\rangle_2 + c_2|\beta\rangle_1|\alpha\rangle_2.$$ (2.13)

Obviously, it is impossible to write this wavefunction in a decomposed form. Actually, what we can predict for the output light is the probability: there is a probability of $|c_1|^2$ of finding $|\alpha\rangle$ in beam 1 and $|\beta\rangle$ in beam 2 and a probability of $|c_2|^2$ of finding $|\beta\rangle$ in beam 1 and $|\alpha\rangle$ in beam 2.
of $|c_2|$ of finding $|\beta\rangle$ in beam 1 and $|\alpha\rangle$ in beam 2, respectively. If we use a 50-50 beamsplitter, the probabilities in both cases are $\frac{1}{2}$.

As an entangled state, a coherent superposition of two orthogonal eigenstates is also called the Schrödinger cat state or macroscopic superposition state. If we assume which state $|\alpha\rangle$ represents a cat which is alive and $|\beta\rangle$ represents a cat that is dead, equation (2.13) will show the entanglement of both alive and dead cats. In a strict interpretation of quantum theory, all quantum states represent the probability of occurrence of specific events. A Schrödinger cat state is a typical example: if the Schrödinger cat gedankenexperiment is repeated many times under the condition of $c_1 = c_2$, one half of cats will be found alive and one half will be found dead.

In an atomic system, for example an oxygen atom, the singlet atomic state is an entangled singlet state. If $\alpha$ is a positive electron spin state and $\beta$ is negative electron spin state, the singlet atomic state is then

$$\psi = \frac{1}{\sqrt{2}}[\alpha(1)\beta(2) - \beta(1)\alpha(2)]. \quad (2.14)$$

This atomic state is an entangled state of two electronic spin states. This entangled state is referred to as Schmidt state (Schmidt decomposition), where it is required that $\langle \alpha | \beta \rangle_1 = 0$ and $\langle \alpha | \beta \rangle_2 = 0$, i.e., $\alpha_1$ and $\beta_2$ are orthogonal. This assumption is useful in our studies, since we require that the states in each basis are orthogonal.

This section enables for us to investigate Bell-type cryptographic systems.

### 2.6 EPR NONLOCAL REALISM

We need the following assumption: if there are two small objects, one here on Earth and the other one on Mars, no modification of the properties of the object
on Earth will occur due to an interaction of the object on Mars with a third body also located on Mars. However, according to Einstein, Podolsky and Rosen (EPR), this assumption is false.

In 1935, Einstein, Podolsky and Rosen developed the theory of so-called local realism [27], which raises a fundamental question of quantum mechanics: can the quantum-mechanical description of physical reality be considered complete? Their argument is usually called the Einstein-Podolsky-Rosen paradox. The essence of the paradox is concerned physical reality. They wrote their famous reality criterion: *If, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity.*

When a single quantum object is considered, it is impossible to measure its position $x$ and momentum $p$ simultaneously without substantial errors, using the commutation relation $[x, p] = \hbar/i$ (note that for convenience $\hbar$ is ignored). Physically, when $p$ is measured and a definite value obtained, a previous element of reality corresponding to $x$ is destroyed.

However, according to EPR, things change dramatically, when two correlated quantum objects ($\alpha$ and $\beta$) are considered. They were able to show that

$$[x_\alpha - x_\beta, p_\alpha - p_\beta] = 0$$

and find an entangled wave function

$$\Psi = \delta(x_\alpha - x_\beta - L)\delta(p_\alpha + p_\beta),$$

where $L$ is a large distance beyond the range of mutual interaction of the particles. In state $\Psi$, we know only the total momentum but nothing about the positions of the particles, however if we measure $x_\alpha$, then we are able to predict $x_\beta$ without measuring it. In terms of the EPR criterion, $x_\beta$ corresponds to physical reality.
On the other hand, if we measure $p_x$, we can then obtain the $p_y$ with certainty, without disturbing $\beta$ particle. Again, $p_y$ corresponds to physical reality. Consequently, we find that our measurement is able to provide the values of both position and momentum. This argument contradicts fundamental quantum-mechanical principles.

In fact, the EPR paradox hinges on the examination of the joint quantum-mechanical state of two particles that are initially correlated in such perfect way that a measurement on one of particles immediately tells us the state of the other particle, without any need to measure or disturb the other particle. In 1951, Bohm revealed that the EPR can equally well be stated in terms of two particles of spin-$\frac{1}{2}$ in a state of net spin zero, which is a state where the spins of the two particles are opposite.

Consider two particles of spin-$\frac{1}{2}$, such as two electrons with opposite spins. Suppose that the particles are initially close together and move to a large distance. We then measure the spin of one of the particles. Since the total spin is zero, the measurement of the spin of the first particle will tell us the spin of the second particle which must have the opposite spin. If the spin of the first particle is $\frac{1}{2}\hbar$, then the second one must be $-\frac{1}{2}\hbar$. Since we did not touch the second particle, the state remains the same after the measurement. We may use the same method to determine the spin components along $x$ and $y$ directions, and hence all spins can be determined without disturbing the second particle. This contradicts quantum mechanics. The crucial step in the EPR argument hinges on the reality criterion of particles and on the locality of the measurement procedure. The spin of the second particle is supposed to exist in itself, even if it is not measured. In the view of EPR, the state vector must be supplemented or replaced be some extra "local hidden variables." The spin components mentioned previously must be expressed as functions of these hidden variables so that the spin components can
be well defined. Using the assumption of hidden variables, it is possible to obtain agreement with quantum mechanics. However, in 1965, Bell demonstrated that not all of the subtleties of the probabilistic predictions of quantum theory can be duplicated by hidden variables [7].

2.7 BELL'S THEOREM

In 1964, John Bell demonstrated that the correlations among spin measurement on two particles of spin-$\frac{1}{2}$ in a state of zero net spin cannot be duplicated by local hidden variables. Bell’s theory was thought to be the most profound discovery of science.

Now we review Bell’s work. Consider a singlet state, given by the equation (2.14). Suppose that the spin component of particle $\alpha$ is measured along the direction of a unit vector $\vec{a}$ and the spin component of particle $\beta$ is measured along the direction of a unit vector $\vec{b}$. The measured observables are $\vec{\sigma}(\alpha) \cdot \vec{a}$ and $\vec{\sigma}(\beta) \cdot \vec{b}$, where $\vec{\sigma}(\alpha)$ and $\vec{\sigma}(\beta)$ are Pauli spin matrices corresponding to the two particles, where Pauli spin matrix is defined by

$$\vec{\sigma} = \sigma_x \vec{i} + \sigma_y \vec{j} + \sigma_z \vec{k},$$

and

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The results of the measurements are $A$ and $B$, respectively, and can have values $\pm 1$. The quantum mechanical correlation coefficient, in the case of the singlet state is

$$C(\vec{a}, \vec{b}) = \langle \psi | (\vec{\sigma}(\alpha) \cdot \vec{a}) \otimes (\vec{\sigma}(\beta) \cdot \vec{b}) | \psi \rangle. \quad (2.17)$$

It is easy to show that

$$C(\vec{a}, \vec{b}) = -\vec{a} \cdot \vec{b} = -\cos \theta. \quad (2.18)$$
Bell examined this correlation coefficient for measurement of the spin components along three directions. He proved that in any local hidden-variable theory the correlation coefficient is restricted by an inequality which contradicts quantum mechanics.

Consider three different directions specified by the unit vectors $\vec{a}$, $\vec{b}$ and $\vec{c}$. We now perform sequential paired measurements, along the directions $\vec{a}$ and $\vec{b}$, the directions $\vec{a}$ and $\vec{c}$ and the directions $\vec{b}$ and $\vec{c}$. The correlations corresponding to this sequence of measurements are: $C(\vec{a}, \vec{b})$, $C(\vec{a}, \vec{c})$, and $C(\vec{b}, \vec{c})$. According to local hidden-variable theory, the expectation values of these correlation functions are averages over the local hidden variables, with some distribution function. Bell proved that in the theory of local hidden variables the correlation coefficients must obey the inequality

$$S_1 = |C(\vec{a}, \vec{b}) - C(\vec{a}, \vec{c})| - C(\vec{b}, \vec{c}) \leq 1.$$  \hspace{1cm} (2.19)

Note that this is independent of the details of hidden-variable theory. This result is called Bell's inequality and does not conform with quantum mechanics. For example, choosing $C(\vec{a}, \vec{b}) = -\cos \frac{\pi}{4}$, $C(\vec{a}, \vec{c}) = -\cos \frac{\pi}{2}$, $C(\vec{b}, \vec{c}) = -\cos \frac{\pi}{4}$, we have $S_1 = \sqrt{2}$ for quantum mechanics (without using the hidden-variable theory).

A more general form of the inequality due to Clauser et al. is called CHSH inequality [28], considers four different directions instead of three. They defined the quantity, called Bell's quantity,

$$S_2 = |C(\vec{a}, \vec{b}) - C(\vec{a}, \vec{b'})| + |C(\vec{a'}, \vec{b}) + C(\vec{a'}, \vec{b'})|,$$  \hspace{1cm} (2.20)

where two orthogonal unit vectors $\vec{a}$ and $\vec{a'}$ are associated with the particle $\alpha$ and two orthogonal unit vectors $\vec{b}$ and $\vec{b'}$ are associated with the particle $\beta$. Suppose that their orientations are found by clockwise rotations of $\pi/4$ in the order $\vec{a}, \vec{b}, \vec{a'}, \vec{b'}$. It can be showed that with quantum mechanics,

$$S_2 = |\vec{a} \cdot \vec{b} - \vec{a} \cdot \vec{b'}| + |\vec{a'} \cdot \vec{b} + \vec{a'} \cdot \vec{b'}| = 2\sqrt{2}.$$  \hspace{1cm} (2.21)
However using the theory of hidden variables, we can obtain,

$$S_2 = |\vec{a} \cdot \vec{b} - \vec{a} \cdot \vec{b}'| + |\vec{a}' \cdot \vec{b} + \vec{a}' \cdot \vec{b}'| \leq 2.$$  \tag{2.22}

This form of Bell's inequality is commonly used by researchers.

Bell's inequality can also be derived for correlation of polarized photon pairs. The first EPR gedankenexperiment using polarized photon pairs was based on Bohm's theory [4] and was performed by Aspect, Granier and Rodger [5]. Their work provides a basic model for the first EPR version of quantum cryptography which was developed by Ekert [13]. A schematic diagram for the experiment is shown in figure 2.5. A source labeled by $S$ generates two-photon states. For each pair of photons, after the photons are separated, one photon (say, photon 1) is launched towards analyzer 1 and the other one (say, photon 2) is launched towards analyzer 2 for correlation measurements of their polarizations along arbitrary directions $\vec{a}$ and $\vec{b}$. Each measurement can yield either the result 1 (if the polarization is found parallel to the measuring vector) or $-1$ (if the polarization is found perpendicular to the measuring vector).

Suppose $P_{\pm\pm}$ denote the probabilities of obtaining the result $\pm 1$ along $\vec{a}$ (photon 1) and $\pm 1$ along $\vec{b}$ (photon 2). The correlation coefficient of the measurements is defined by

$$C(\vec{a}, \vec{b}) = P_{++}(\vec{a}, \vec{b}) + P_{--}(\vec{a}, \vec{b}) - P_{+-}(\vec{a}, \vec{b}) - P_{-+}(\vec{a}, \vec{b}),$$  \tag{2.23}

which is the sum of all probabilities for the measurements. Using this correlation coefficient, we can construct Bell's quantity (2.20). Theoretically, under the
criterion of the local reality, it should be possible demonstrate Bell’s inequality. However, like other experiments, the results of their experiment showed a strong violation of Bell’s inequality.

In 1991, Ekert, for the first time, applied Bell’s theory to quantum cryptography. His model is similar to the experiment by Aspect et al.. He believed that eavesdropping is equivalent to adding a local hidden variable to the system, hence, in principle, nonviolation of Bell’s inequality can be used to reveal an attempt at eavesdropping.
When the medium of communication involves quantum-mechanical particles, the system naturally obeys quantum-mechanical laws. One important feature of such a system is the existence of uncertainty, which, as we have mentioned in the last chapter, is basically due to the wave-particle property. Using quantum-mechanical particles to carry information, an eavesdropper may be prevented from obtaining the information sent by the sender. Bennett and Brassard are the researchers who first brought us a practical cryptographic protocol based on Heisenberg's uncertainty in quantum mechanics. In this chapter we review the BB protocol and investigate a novel model, quantum cryptographic protocols using an optical coupler. Our protocol is based on the theory of quadrature phase amplitudes of light. The main result of this protocol has been published in Optics Communications.[24]

3.1 BB PROTOCOL

In the late 1960's, Wiesner had the idea of using uncertainty in cryptography, but he did not publish his idea until 1983 [1]. One of his ideas was to use a stream of polarized photons to transmit two messages (corresponding to two quantum-mechanical states). Depending upon the choice of the detectors by the receiver, only one message can be readable. Bennett and Brassard, following Wiesner's
idea, developed a quantum cryptographic protocol which was published in 1982 [2] (we here call it the BB protocol). Subsequently, Bennett and his co-workers successfully built a quantum cryptographic apparatus at the IBM T. J. Watson Research Laboratory, USA [6].

The BB protocol shows that information can be encoded in one of four nonorthogonal quantum states based on two bases, in such a way, that any attempt to extract information by an eavesdropper will randomize, and hence destroy the information.

The quantum cryptographic communication in the BB protocol involves two users, say Alice and Bob, who share no secret information, together with an adversary Eve who eavesdrops on their communications. According to the BB protocol, there are orthogonal and closed bases $B_1 = \{ | \rightarrow \rangle, | \uparrow \rangle \}$ and $B_2 = \{ | \swarrow \rangle, | \nwarrow \rangle \}$ related to different polarizations: rectilinear and diagonal (or using circular basis, see Chapter 2). In order to measure these states, we introduce two quantum-mechanical operators, $\hat{O}_{B_1}$ and $\hat{O}_{B_2}$, such that

\begin{align}
\hat{O}_{B_1} | \rightarrow \rangle &= \mu_0 | \rightarrow \rangle, \quad \hat{O}_{B_1} | \uparrow \rangle = \mu_1 | \uparrow \rangle, \\
\hat{O}_{B_2} | \swarrow \rangle &= \nu_0 | \swarrow \rangle, \quad \hat{O}_{B_2} | \nwarrow \rangle = \nu_1 | \nwarrow \rangle,
\end{align}

where the eigenvalue $\mu_0$ or $\nu_0$ denotes the binary code "0" and the eigenvalue $\mu_1$ or $\nu_1$ denotes binary code "1". $\hat{O}_{B_1}$ and $\hat{O}_{B_2}$ do not commute, i.e. $[\hat{O}_{B_1}, \hat{O}_{B_2}] \neq 0$. This leads to the uncertainty in measurement described by Heisenberg's uncertainty principle

\begin{equation}
\langle \Delta \hat{O}_{B_1}^2 \rangle \langle \Delta \hat{O}_{B_2}^2 \rangle > 0;
\end{equation}

which suggests that a measurement on any state using an incorrect basis will be uncertain. The uncertainty can in fact be interpreted from the following. Since the states in $B_1$ and $B_2$ are orthonormal and complete, respectively, we have

\begin{equation}
| \rightarrow \rangle = c_1 | \swarrow \rangle + c_2 | \nwarrow \rangle,
\end{equation}
Table 3.1 The BB key distribution protocol for the process of sending/receiving between Alice and Bob. (1) Alice sends a random sequence of photons polarized along four directions based on $B_1$ and $B_2$. (2) Bob measures the photons in a random sequence of bases. (3) Bob's measurements are obtained. (4) Bob tells Alice which basis he has used for each pulse he received. (5) Alice tells which basis he used was correct. (6) Binary information for the key distribution is obtained.

<table>
<thead>
<tr>
<th>1:</th>
<th>$\uparrow\rangle$</th>
<th>$\downarrow\rangle$</th>
<th>$\rightarrow\rangle$</th>
<th>$\uparrow\rangle$</th>
<th>$\downarrow\rangle$</th>
<th>$\rightarrow\rangle$</th>
<th>$\uparrow\rangle$</th>
<th>$\rightarrow\rangle$</th>
<th>$\uparrow\rangle$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2:</td>
<td>$O_{B_1}$</td>
<td>$O_{B_2}$</td>
<td>$O_{B_2}$</td>
<td>$O_{B_1}$</td>
<td>$O_{B_1}$</td>
<td>$O_{B_2}$</td>
<td>$O_{B_2}$</td>
<td>$O_{B_1}$</td>
<td>$O_{B_1}$</td>
</tr>
<tr>
<td>3:</td>
<td>$\rightarrow\rangle$</td>
<td>$\rightarrow\rangle$</td>
<td>$\rightarrow\rangle$</td>
<td>$\rightarrow\rangle$</td>
<td>$\rightarrow\rangle$</td>
<td>$\rightarrow\rangle$</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4:</td>
<td>$O_{B_1}$</td>
<td>$O_{B_2}$</td>
<td>$O_{B_1}$</td>
<td>$O_{B_2}$</td>
<td>$O_{B_1}$</td>
<td>$O_{B_2}$</td>
<td>$O_{B_1}$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5:</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6:</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\[
| \uparrow\rangle = c_3| \uparrow\rangle + c_4| \downarrow\rangle, \quad (3.5)
\]
\[
| \rightarrow\rangle = c_5| \rightarrow\rangle + c_6| \uparrow\rangle, \quad (3.6)
\]
\[
| \downarrow\rangle = c_7| \rightarrow\rangle + c_8| \uparrow\rangle, \quad (3.7)
\]

where $c_i$ are coefficients of the expansions. If we use a wrong operator in a measurement, say, $O_{B_2}| \rightarrow\rangle$, we then have a probability of $|c_1|^2$ of obtaining $| \rightarrow\rangle$ and a probability of $|c_2|^2$ of obtaining $| \downarrow\rangle$. It is similar for the other states.

The BB protocol starts with Alice, who sends a random sequence of all four canonical kinds of polarized photons to Bob. Bob randomly and independently chooses one of the measuring bases to measure each photon pulse. They discuss publicly the bases Bob has used and discard those which disagree and keep secret the photon polarization outcome. The remaining photons can then be used to construct a secret key. Any eavesdropping attempt to extract information will irretrievably destroy some information since basis information was unknown to Eve before Alice and Bob completed the transmission. Eavesdropping causes a
change in the information flow between Alice and Bob, and hence reveals the presence of the eavesdropper. A more detailed interpretation of the BB protocol is shown in Table 3.1.

If we use photon states which are not pure single photon states, there is the potential for a beamsplitting attack. A light pulse with two photons will possibly release all the information to an eavesdropper who uses an appropriate beamsplitting techniques, for example, a multi-beamsplitter attack. In figure (3.1), we proposed such an eavesdropping technique. The main beamsplitter extracts a small fraction of the photons (say, two photons), letting the remainder pass undisturbed to Bob. Each fraction from the beamsplitter is split (via a 50/50 beamsplitter) into two beams that are then measured using different bases. Eve records each measurement and determines which basis is correct only after the correct bases are announced publicly. Consequently, Eve obtains the perfect information she needs without being detected by Alice and Bob.

In fact, polarization of a multiphoton state in the BB protocol can be detected using an approach of dividing/regrouping, without prior knowledge of the measuring basis. The photon pulse sent by Alice can be divided into several fractions,
which are then regrouped into two groups, group one and group two. Each group contains several small pulses or fractions. We can arbitrarily choose detectors, either $\hat{O}_{B_1}$ or $\hat{O}_{B_2}$ for each group, for example, we use $\hat{O}_{B_1}$ to measure the pulses in group one and $\hat{O}_{B_2}$ to measure the pulses in group two. It is certainly that one of detectors is used wrongly. This wrong detector can be readily found, since it leads to uncertain results (both 0 and 1). On the other hand, we will see that the correct detector gives a sure result. Therefore, the polarization of the extracted photon pulse can be accurately determined.

The BB protocol (and most other quantum protocols) requires single-photon states to avoid beamsplitting attacks. However, in practice it is difficult to produce a light pulse containing only one photon (although it was demonstrated in the laboratory [29]). It is much easier to produce a coherent pulse which is a superposition of one, two, ... photon states. In order to use currently available techniques, we can choose very faint photon pulses so the average photon number, $\langle n \rangle$, is substantially smaller than one, then there is a probability of $\langle n \rangle^2/2$ that an eavesdropper will be able to split the pulse into two or more photons.

### 3.2 QUANTUM CRYPTOGRAPHY USING FOUR NONORTHOGONAL STATES

#### 3.2.1 Physical background

Since our protocol appears to be substantially different from that using polarized photons, we should explain the relationship between uncertainty and quantum measurement.

For a quantum field mode $c$, we can write it in the form of $c = c_1 + ic_2$, where $c_1$ and $c_2$ are quadrature phase amplitudes. The inequality of uncertainty for the
quadrature phase amplitudes is given by

\[ \langle \Delta c_1^2 \rangle \langle \Delta c_2^2 \rangle \geq 1/16. \]  (3.8)

where \( \langle \Delta c_1^2 \rangle \) (\( \langle \Delta c_2^2 \rangle \)) denotes the variance of \( c_1 \) (\( c_2 \)). Inequality (3.8) suggests that only one of two quadrature phase amplitudes can be accurately determined for one measurement.

For a squeezed state which is a minimum uncertainty state, the equality of (3.8) will hold, while the variance of one of the quadrature components is squeezed (to zero for a perfect squeezed state) and the variance of the other quadrature component is enlarged (to infinity for a perfect squeezed state). For convenience, we assume that \( \xi \) is a squeezing mode. An ideal squeezed state is evolved from a vacuum state \( |0\rangle \) by operation with the squeezing operator

\[ S(\xi) = \exp(\frac{1}{2}\xi^*b^2 - \frac{1}{2}\xi b^\dagger^2), \]

followed by operation with the displacement operator

\[ D(\beta) = \exp(\beta b^\dagger - \beta^*b), \]

i.e.,

\[ |\mu \nu \beta\rangle = D(\beta)S(\xi)|0\rangle, \]  (3.9)

where \( \beta \) is the amplitude of mode \( b \), \( \xi = r \exp(i\theta) \), \( |\mu|^2 = \cosh^2 |r| \), and \( |\nu|^2 = \sinh^2 |r| \). \( r \) denotes a squeezing parameter. The variances of quadrature phase
In planes of quadrature-phase amplitudes, (a) shows Alice's encoding strategy based on four nonorthogonal coherent states; (b) shows Bob's tap-fibre modes using squeezed light. Uncertainty of a state is represented by error ellipses for squeezed states and by error circles for coherent states.

Amplitudes can be described by

$$\langle \Delta b_1^2 \rangle = \frac{1}{2} e^{-2r}, \quad \langle \Delta b_2^2 \rangle = \frac{1}{2} e^{2r}. \quad (3.10)$$

As showed in figure 3.3 (b), two orthogonal squeezed states are used by Bob as his input to the optical coupler. The mode $b_E = b_1$ corresponds to $r >> 0$, while the mode $b_N = i b_2$ corresponds to $r << 0$. One advantage of using squeezed light is that one of quadrature components can be measured with little influence of quantum noise.

The area of ellipse for a mode represents uncertainty (or noise), for instance, we can see that, for the squeezed mode $b_E = b_1$ the $x$ component (the projection on $x$ axis) is knowable (small noise, ideally zero), but the $y$ component (the projection on $y$ axis) is uncertain (large noise, ideally infinity). We can explain the other mode similarly.

For a coherent state, since the photon distribution is Poissonian, the uncertainties for both quadrature-phase amplitudes are equal and the equality in (3.8) also holds. Hence both variances of the quadrature phase amplitudes are $1/4$. Accordingly, in figure 3.3 (a) we can see a noise circle for each coherent state, where
we have assumed that mode $a$ represents a coherent state with four encoding arrangements $a_E = a_1$, $a_W = -a_1$, $a_N = ia_2$, and $a_S = -ia_2$ (east, west, north, and south states). Under our encoding strategy, overlaps among these states should be as large as possible, thus it is accordingly assumed that the overlap between the east and west states is approximately 65%, so does the overlap between the north and south states. This requires that the mean number of photons for each state should be around 0.1. The absolute magnitude of overlap of two coherent states can be calculated by

$$|\langle \alpha | \beta \rangle|^2 = e^{-|\alpha - \beta|^2}. \tag{3.11}$$

Using this formula, it is easy to find that the overlap between the east and west state or the north and south states is 65%, and between the east and north states is around 82% (the same for each other pairs of neighbour states).

When a state is subject to an overlap between two states, it will not be able to be determined for sure because it could belong to either of these states. When a state is not in the overlap region, it will be possibly determined without mixing with other states. Since under our arrangement total area of overlaps in a state is more than 90% and a large fraction of area has four overlap layers, it is almost impossible to obtain a certain result when performing a measurement on these states.

A homodyne detection is the most sound scheme for performing a measurement on a quadrature phase amplitude. The value of measurement is actually equal to the projection on the axis of the corresponding detector. We may lock a homodyne detector to an orientation, $x, -x, y,$ or $-y,$ which suits the measurements for different encodings, and consistently, we define four detection vectors $V_x, V_{-x}, V_y,$ or $V_{-y},$ which in fact are four noncommuting projection operators.
We first look at a homodyne detection performed on a single coherent state, the east state or the north state, and ignore the superposition for a while. In order to measure the east state, the homodyne detector must be locked at \( x \) direction (i.e., using \( V_x \)). This is because it has the largest probability of obtaining the correct result — a value of the mean \( \langle a_1 \rangle \), despite the uncertainty \( \langle \Delta a_1^2 \rangle = 1/4 \). When utilizing the same projection operator \( V_x \) to detect the north state, we will then be unable to obtain a correct value, but have a high probability of obtaining zero (the uncertainty also equals \( 1/4 \)). On the other hand, if a state does not have any projection on the detection vector, the state will not be able to be determined. For example, using \( V_x \), we cannot determine the west state, since it does not have any useful projection on \( V_x \) (except the projection due to noise). It is concluded that for obtaining a correct detection the detection vector must be set accordingly to the direction of the signal state.

Since we are using four nonorthogonal states and each state has a large area of overlap with other states, it is hardly possible to correctly determine one out of these states by use of a homodyne detector. This feature presents a promise for us to apply these states to cryptography.

As shown in figure 3.2, on the receiving side, we employ an optical coupler which consists of two optical fibres. Alice’s signal mode is expressed by a creation operator \( a^\dagger \) or an annihilation operator \( a \). Bob’s mode in the tap fibre is represented by a creation operator \( b^\dagger \) or an annihilation operator \( b \). For an optical coupler with coupling constant \( \kappa \), the quantum fields after the coupling obey [30]

\[
a' = (1 - \kappa)^{1/2}a + \kappa^{1/2}b, \tag{3.12}
\]

\[
b' = -\kappa^{1/2}a + (1 - \kappa)^{1/2}b, \tag{3.13}
\]

where \( 0 \leq \kappa \leq 1 \). \( \kappa = 0 \) corresponds to no signal having been exchanged between the fibres, while \( \kappa = 1 \) corresponds to a complete signal having been exchanged
between the fibres. The corresponding field quadrature operators are

\begin{align}
a_1 &= \frac{a + a^\dagger}{2}, \quad a_2 = \frac{a - a^\dagger}{2i}, \\
b_1 &= \frac{b + b^\dagger}{2}, \quad b_2 = \frac{b - b^\dagger}{2i}.
\end{align}

(3.14) (3.15)

The explicit expression for quadrature components for coupled states can be obtained in terms of Equations (3.12)-(3.15). After coupling the mean number of photons at port one is given by

\begin{equation}
\langle a'^\dagger a' \rangle = (1 - \kappa)\langle a'^\dagger a \rangle + \kappa\langle b'^\dagger b \rangle + \sqrt{(1 - \kappa)\kappa}\langle a'^\dagger b \rangle + \langle b'^\dagger a \rangle), \tag{3.16}
\end{equation}

and at port two is given by

\begin{equation}
\langle b'^\dagger b' \rangle = \kappa\langle a'^\dagger a \rangle + (1 - \kappa)\langle b'^\dagger b \rangle - \sqrt{(1 - \kappa)\kappa}\langle a'^\dagger b \rangle + \langle b'^\dagger a \rangle), \tag{3.17}
\end{equation}

3.2.2 Shared cryptographic bits

The basic intention is to establish a common key between two parties, Alice and Bob, who share no secret information at the beginning of the cryptographic communication. The optical coupler is controlled by Bob who can independently choose his own squeezed input source for it. Both signal generators are controlled by a time base that guarantees a perfect photon coupling. The output signal is detected using two homodyne detectors, one for each port. Also, importantly, in order to realize a perfect coupling, Alice and Bob also need to choose a phase reference before their communication starts. This can be done by Alice sending a sequence of bright reference pulses to Bob and publicly announcing their phase.

Alice's generator produces faint coherent light, on the average, 0.1 photon per pulse, i.e., \( \langle a'^\dagger a \rangle = 0.1 \). As we have mentioned, under this assumption the total overlap on a state is over 90%. The probability a signal pulse contains one or more photon is approximately 10%. This figure suggests that 90% of the total pulses are vacuum states. Note that it is possible to employ weaker signal light
Table 3.2 The results of the photon coupling. The illustration is based on a quadrature plane. We have assumed equal intensity for both mode $a$ and mode $b$, the symbol "x" represents "discarded", C represents "Canceled", E represents "Enhanced", and a sign, character or binary figure in front of "/" has a higher probability of appearance. In other words, those in front of "/" are correct; those behind "/" are associated with the overlap on the corresponding opposite state. The later ones can be corrected eventually.

<table>
<thead>
<tr>
<th>Alice</th>
<th>Bob</th>
<th>Coupling Result</th>
<th>Measurement</th>
<th>Final Result</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Vector</td>
<td>Status</td>
</tr>
<tr>
<td>$a_E$</td>
<td>$b_E$</td>
<td>$a' = \frac{1}{\sqrt{2}}[(+/-)a_1 + b_1]$</td>
<td>$V_x$</td>
<td>E/C</td>
</tr>
<tr>
<td></td>
<td>$b_N$</td>
<td>$a' = \frac{1}{\sqrt{2}}[(+/-)a_1 + i b_2]$</td>
<td>$V_y$</td>
<td>Uncertain</td>
</tr>
<tr>
<td>$a_W$</td>
<td>$b_E$</td>
<td>$a' = \frac{1}{\sqrt{2}}[(+/-)a_1 + b_1]$</td>
<td>$V_x$</td>
<td>C/E</td>
</tr>
<tr>
<td></td>
<td>$b_N$</td>
<td>$a' = \frac{1}{\sqrt{2}}[(+/-)a_1 + i b_2]$</td>
<td>$V_y$</td>
<td>Uncertain</td>
</tr>
<tr>
<td>$a_N$</td>
<td>$b_E$</td>
<td>$a' = \frac{1}{\sqrt{2}}[b_1 + (+/-)ia_2]$</td>
<td>$V_x$</td>
<td>Uncertain</td>
</tr>
<tr>
<td></td>
<td>$b_N$</td>
<td>$a' = \frac{1}{\sqrt{2}}[b_1 - (+/-)ia_2]$</td>
<td>$V_x$</td>
<td>Uncertain</td>
</tr>
<tr>
<td>$a_S$</td>
<td>$b_E$</td>
<td>$a' = \frac{1}{\sqrt{2}}[b_1 - (+/-)ia_2]$</td>
<td>$V_x$</td>
<td>Uncertain</td>
</tr>
<tr>
<td></td>
<td>$b_N$</td>
<td>$a' = \frac{-1}{\sqrt{2}}[(+/-)a_2 - b_2]$</td>
<td>$V_y$</td>
<td>C/E</td>
</tr>
</tbody>
</table>

such that the superposition of the four nonorthogonal states can be even larger, however we do not intend to do that, since our assumption is sufficient for our
cryptographic protocol. Bob’s squeezed light is much brighter and has on the average one photon per pulse.

Our quantum cryptographic key distribution protocol is described as follows:

1: Assuming that \( \alpha_i \) is randomly selected from four quantum states \( a = \{a_E, a_W, a_N, a_S\} \), Alice constructs a vector \( A = (\alpha_1, \alpha_2, ..., \alpha_n) \), where \( \alpha_i \in a = \{a_E, a_W, a_N, a_S\} \). \( a \) is public information, while \( A \) is private data only known by Alice.

2: Bob independently chooses a vector \( B = (\beta_1, \beta_2, ..., \beta_n) \) of \( n \) random states, \( \beta_i \in b = \{b_E, b_N\} \). \( b \) is public information, but \( B \) is private data only known by Bob.

3: Alice sends \( \alpha_i \in A \) to Bob, while Bob injects a \( \beta_i \) which interacts with \( \alpha_i \) in Bob’s optical coupler. The coupling result is shown in Table 3.2. In terms of the subsequent detection, Bob sets \( \beta'_i = \begin{cases} 0 & \text{a bright flash at Port 1 and nothing at Port 2,} \\ 1 & \text{a bright flash at Port 2 and nothing at Port 1,} \end{cases} \)

otherwise, Bob deletes the bit. Alice and Bob repeat the process until the whole signal string is sent. “bright flash” means that two photons have been projected on Bob’s detection vector. Bob’s method can be summarized as a screening criterion: An output bit from the optical coupler is recorded, if and only if Bob finds that two photons are projected on the detector at one port and nothing is projected on the detector at the other port. This criterion solves the problem caused by noise. Bob’s measurements are based on a homodyne detection scheme, where both detectors are arranged in terms of the tap-fibre mode used by Bob himself. If the tap-fibre mode is based on \( b_E \), both detectors should also be set toward the \( x \) direction; if the tap-fibre mode is based on \( b_N \), both detectors should be set up toward the \( y \) direction.
4: Bob keeps $B$ and $B' = (\beta_1', \beta_2', ..., \beta_n')$ secret. Alice keeps $A$ secret.

5: Bob speaks to Alice publicly for each $\beta_i'$: *Accept* if Bob "saw" a bright flash at Port 1 (2) and nothing at Port 2 (1) (obeying the screening criterion); *reject* if Bob "saw" flashes at both ports or other instances which do not satisfy the screening criterion.

6: Since Bob's result contains a large number of flaw bits owing to quantum noise and overlapping, Bob must announce to Alice which detection vector has been used for each accepted bit, but nothing about the outcome of the measurement. Alice asks Bob to detect all bits obtained using an incorrect detection vector, for example, Alice may ask him to detect a north-state-related "0" bit which is obtained by using $V_x$. This step ensures that all flaw bits subject to the overlaps with two closer neighbour states (but not the opposite state) are removed. (We will give more explanation later.)

7: Bob's remaining bits still contain a large fraction of flaw bits subject to overlap with the opposite states. In order to correct (but not remove) the flaw bits, the following steps should be taken:

- Alice secretly divides all remaining bits related to each state, east, north, west, or south into $N$ groups ($N \geq 100$), where each group contains $m$ ($m \geq 30$) bits. This requires that the number of original signal bits sent by Alice are sufficient. Each group involves only one signal state, but both binary bits. Amongst these binary bits, one fraction of binary bits ("0" or "1") stems from the correct detections and these bits are the majority; the other group of binary bits ("1" or "0") come from the overlap on the opposite state. Note that during the grouping the original positions of the bits were not changed.

- Alice publicly announces the grouping result, without releasing any encoding information. So nobody knows which group belongs to which
state, except Alice herself. Since each Bob’s detection vector has been used to two nonorthogonal states, knowing the detection vector of each group releases not encoding information of the group.

- Bob calculates the number of “0” or “1” bits in each group. The encoding of the majority bits will represent the encoding of all bits in the group. For example, if Bob finds that “0” bits are the majority, he will regard all bits in the group as “0”.

- Bob tells Alice the positions of all useful bits. Alice knows the full information of these bits.

8: Alice and Bob keep the bits which have eventually survived as the secret key.

Table 3.2 shows all possible detection results in Bob’s coupler when both light pulses have the same intensity. Instead of illustrating all cases in the table, we only focus on the first case, where Alice uses the east state $a_E$. The explanations for the remaining cases are similar. When Bob uses $b_E$ (consistently use $V_x$), according to the coupling equations, there are two possible outcomes: (1) The output at port 1 is enhanced and the output at port 2 is reduced to a vacuum state due to the cancellation. Bob then further checks whether the outputs satisfy the screening criterion. If the answer is yes, a “0” is accordingly recorded. (2) Because of the superposition between the east state and the opposite west state, a large fraction of bits associated with the east state turn out to be mixed with the west state, and Bob could then have a false result, i.e. a “1” could be recorded. The late bit is obviously wrong, but Bob does not realize his mistake. In order to overcome this problem, Alice uses the error correcting method described in the protocol. The mechanism of this error correcting method is simple: since the
overlap between the states is not 100%, there is a larger probability of obtaining
the east state rather than the west state. This is obviously true, because only if
the superposition is 100%, the probability of obtaining the east state or the west
state is 1/2,

By means of a Q-representation, we can further explain the error correcting
method. A coherent state \( \alpha \) in a Q-representation is given by

\[
Q(\gamma) = \frac{1}{\pi} e^{-|\gamma - \alpha|^2},
\]

which actually represents a quasi-probability of the coherent state. For the east
coherent state with an average projection value of 0.33 (an intensity of 0.1 photon)
on the \( x \) axis (on the quadrature phase plane), the probability of a projection
being around 1 on a small region \((\Delta x) \cdot y\), where \(-\infty < y < \infty\), is given by

\[
P(\text{projection} = 1 | \alpha = 0.33) = \frac{1}{\sqrt{\pi}} e^{-0.637^2} \Delta x \approx 0.36 \Delta x,
\]

while the probability of projection being \(-1\) on the small region is given by

\[
P(\text{projection} = -1 | \alpha = 0.33) = \frac{1}{\sqrt{\pi}} e^{-1.33^2} \Delta x \approx 0.0963 \Delta x.
\]

It is easy to find that, amongst total pulses with a value 1 or \(-1\) projection on
\( x \) axis, the 1-pulses is 79% and the \(-1\)-pulses 21%. According to these data, we
may roughly calculate the correctness rate of Bob's error correcting: assuming
that \( m = 30 \) and the minimal number of bits \( m_{\min} \) for Bob to correctly identify
the encoding is greater than \( m/2 = 15 \), we have the correctness rate:

\[
P(m_{\min} > m/2) = 1 - \sum_{i=1}^{m} \binom{m}{i} (0.79)^i (0.21)^{m-i} \approx 0.9996.
\]

This value suggests that Bob is almost 100% correct. Note however that if an
eavesdropper wants to measure the signal, she cannot have such a high ratio of
1-pulses to \(-1\)-pulses, since her detection is subject to the superposition from
other two neighbour states, the north and south states. Bob does not have this
problem, because Alice can ask him to delete all bits owing to the superposition with the two neighbour states. This case will be further studied in next section.

We now focus on the second case, i.e., Alice still uses \( a = a_1 \) and Bob uses the other mode \( b_N \) (consistently uses \( V_y \)). Bob is obviously wrong. Most possibly, the outputs at one or both ports are nonzero, Bob can thus "view" a light flash with a various intensity at one or both ports. These bits are useless and can be removed in terms of the screening criterion. However, since the measurement is subject to the noise or overlaps, we must consider that Bob might occasionally obtain a result which meets the screening criterion. When this happens, Bob will not be able to identify the flaw. In order to get rid of these flaw bits, no matter what measurement result has been obtained, Alice will ask Bob to delete the bits.

We have not explained the influence of overlaps associated with the two neighbour states, the north and south states. These instances actually belong to other two case where Alice sends the north or south state. The corresponding flaw bits will be handled by Alice and Bob using a similar procedure given above.

### 3.2.3 Eavesdropping

Assume that there is an adversary called Eve who attempts to eavesdrop on Alice and Bob’s communication. Eve can launch an intercept/resend attack. The first method Eve could choose is to measure the intercepted signal by using a similar optical coupler. If she does so, at least half of her measurements will be random, because she has to randomly select her tap-fibre states and detection vectors. Moreover, the remaining half of Bob’s measurements are also uncertain due to the superposition of Alice’s signal. Therefore, it is impossible for Eve to regenerate and resend the signal to Bob, using her own measurement.
Assume that Eve knows that four projection operators, \(\{V_x, V_y, V_{-x}, \text{ and } V_y\}\), can be used to detect Alice's signal and these detection vectors respectively suit detecting \(a_E, a_W, a_N, \text{ and } a_S\). Eve might then wish to use her detector to measure Alice's signal directly, instead of using an optical coupler. However, since she does not know which state has been sent by Alice, she has no better way than to choose a detection vector randomly. The probability of choosing the correct detection vector is obviously \(1/4\). Fortunately, even if she happens to select the correct detector, her measurement is still uncertain because of the overlap of the encoding states. If Eve has a correct detection vector and knows that a projection of value 1 is important, it is not hard to find there is a probability of \(3/5\) for her to obtain a wrong projection belonging to the neighbour states. These bits cannot be identified by Eve. The total success rate of measuring a bit is found to be \(1/10\), which suggests that there is little chance of Eve succeeding.

Eve may not do anything but just listens to Alice and Bob's public conversation. After Alice and Bob's implementation of the protocol is complete, Eve is aware which detection vector has been used, which bits were accepted, and which the detection vector has been applied to each group chosen by Alice. Because each detection vector corresponds to two nonorthogonal states, Eve can only guess whether the bits in each group belong to either "0" or "1". Hence, for each individual group, Eve has a \(1/2\) chance to succeed. However, since the number of groups \(N > 100\), Eve's success rate will be less than \(1/2^{400}\) or approximately \(1/10^{120}\). In practice, it is highly unlikely for Eve to succeed.

### 3.2.4 Signal to noise ratio

We now turn our attention to the signal to noise ratio. We study the coupling quadrature amplitude \(a'_4\). The other cases are similar. By averaging over the signal we find that the ratio of the intensity signal to noise for homodyne detection
in coupling mode $a'_1$ is

$$SNR = \frac{\langle a'_1 \rangle^2}{\langle \Delta a'_1 \rangle^2} = \frac{\left[ (1 - \kappa)^{1/2} \langle a_1 \rangle + \kappa^{1/2} \langle b_1 \rangle \right]^2}{(1 - \kappa) \langle \Delta a_1^2 \rangle + \kappa \langle \Delta b_1^2 \rangle}$$  \hspace{1cm} (3.22)

where only bright output pulses are considered (according to the screening criterion, only output at one port is bright).

Because the tap-fibre mode is controlled by Bob, Bob can use a specific photon source. In particular, Bob can use squeezed light. One quadrature component (say $a_1$) of the field has smaller fluctuations than the other quadrature component (say $a_2$), in terms of the uncertainty principle. Explicitly, $\langle \Delta a_1^2 \rangle < 1/4$ and $\langle \Delta a_2^2 \rangle > 1/4$. Using the quadrature component with smaller noise can greatly improve the signal to noise ratio of the system.

We focus on the signal to noise ratio in which mode $b$ is a squeezed state and mode $a$ is a coherent state. The noise observed in detection comes from both the signal mode sent by Alice ($a$) and the auxiliary tap-fibre mode ($b$). If the intensity for both modes is equal, we obtain the ratio:

$$\frac{SNR_{sq}}{SNR_{coh}} = \left[ 1 - \kappa + \kappa \frac{\langle \Delta b_1^2 \rangle}{\langle \Delta a_1^2 \rangle} \right]^{-1} = 2, \hspace{1cm} (3.23)$$

where $SNR_{sq}$ denotes the signal to noise ratio when the mode $b$ is a perfect squeezed state; $SNR_{coh}$ is the signal to noise ratio both Alice and Bob use coherent light. We have assumed $\kappa = 1/2$. It is found that a doubling of the signal to noise ratio has been obtained.

3.3 CONCLUSION

We have summarized the BB protocol and presented a quantum cryptographic system based on the optical coupler and four nonorthogonal states modeled by using quantized arguments: quadrature phase amplitudes of light field. It will be the first demonstration of the usefulness of quadrature phase amplitudes and
the optical coupler to quantum cryptography. We have also showed that the communication efficiency can be improved by using squeezed light to the tap fibre. Photon attenuation has not been studied in this paper, however, the protocol proposed in this work also fits the situation when leakage of photons occurs. The reason is simply that Bob can discard all bits which do not satisfy the screening criterion and keep those which satisfy the screening criterion. If the leakage is considerable large, Alice may make her signal a bit stronger, say 0.15 photon on the average. The slightly stronger signal will not make the security worse.
Ekert was the first person to propose that the quantum correlation could be used for quantum cryptography. His invention is an EPR-type apparatus which, based on Bell’s inequality, assures the security in cryptographic communications. In this chapter we use calculations involving Bell’s inequality to study Ekert’s protocol in both photon-based and spin-$\frac{1}{2}$-particle-based systems. These calculations give an independent verification of Ekert’s protocol.

4.1 INTRODUCTION

In the well-known Einstein-Podolsky-Rosen-Bohm gedankenexperiment (EPR) [4, 27], a source emits pairs of spin-$\frac{1}{2}$ particles in a singlet state (or pairs of photons [5]). When a pair of particles leaves the source, one particle travels towards analyzer $A$ while the other travels towards analyzer $B$. The measurement of correlations of their spin components (or polarization for photons) is performed by analyzers along arbitrary directions which can be described by unit vectors $\vec{a}$ and $\vec{b}$. Each measurement of a spin-$\frac{1}{2}$ particle, in the amount of $\frac{1}{2}\hbar$, can yield two opposite results: $+1$ if the spin is found to be parallel with the direction of the analyzer, and $-1$ if opposite to the direction of the analyzer. Under the physical reality criterion [27], such a measurement fulfills Bell’s inequality [7], but violates quantum mechanics.
Ekert envisaged the usefulness of the EPR experiment and Bell’s inequality in secure communications [13]. In the scheme proposed by Ekert, a secure quantum key can be achieved by exploiting the properties of quantum-correlated particles. Any eavesdropper unavoidably adds some local condition which causes the data measured by legitimate users to display no violation of Bell’s inequality, this in turn reveals the attempt at interception.

### 4.2 PHOTON-BASED SYSTEM

We first present a detailed analysis for the photon-based system. A light source controlled by Alice generates a pair of photons with a certain polarization, obeying the rules of the entangled two-photon state or the so-called “non-product state” [31]. One photon travels along the single mode optical fiber towards Bob’s analyzer and the other photon is sent to Alice’s analyzer. The first passes through Bob’s polarization analyzer, emerging in either the horizontal (+) channel, or the vertical (−) channel. Alice’s measurement is similar. The direction of Bob’s analyzer and the direction of Alice’s analyzer are can be rotated at will. The plane of the analyzer is orthogonal to that of the propagation direction of the photons. Let \( a_\pm \) (\( b_\pm \)) be the annihilation operator for the horizontally (+) or vertically (−) polarized mode for the field traveling to Alice’s analyzer (Bob’s analyzer). Using \( n_1, n_2, n_3 \) and \( n_4 \) to denote the numbers of photons in mode \( a_+, a_-, b_+ \) and \( b_- \) respectively, we have the state \( |n_1, n_2\rangle_a |n_3, n_4\rangle_b \). In terms of linear polarizations, the state of the two entangled photons may be written as

\[
|\Psi\rangle = \frac{1}{\sqrt{2}}(|1, 0\rangle_a |1, 0\rangle_b + |0, 1\rangle_a |0, 1\rangle_b).
\]

We have supposed that the light source produces two identical photons each time, that is both Alice’s and Bob’s analyzers receive photons with the same polarization.
The measurement is carried out by rotating Alice’s analyzer by an angle $\theta_1$ or Bob’s analyzer by $\theta_2$. The modes detected are thus orthogonal transformations of the modes of the signal. In Alice’s case,

$$c_+ = a_+ \cos \theta_1 + a_- \sin \theta_1,$$  \hspace{1cm} (4.2)

$$c_- = -a_+ \sin \theta_1 + a_- \cos \theta_1,$$  \hspace{1cm} (4.3)

while in Bob’s measurement, the modes detected are given by

$$d_+ = b_+ \cos \theta_2 + b_- \sin \theta_2,$$  \hspace{1cm} (4.4)

$$d_- = -b_+ \sin \theta_2 + b_- \cos \theta_2.$$  \hspace{1cm} (4.5)

Note that $\theta_1$ and $\theta_2$ are actually the angles between the photon polarization and the direction of the corresponding analyzer, respectively.

Consider the correlation functions:

$$E(\theta_1, \theta_2) = \frac{\langle (I_1^+ - I_1^-)(I_2^+ - I_2^-) \rangle}{\langle (I_1^+ + I_1^-)(I_2^+ + I_2^-) \rangle}. \hspace{1cm} (4.6)$$

where $\langle I_1^\pm \rangle$ and $\langle I_2^\pm \rangle$ are the intensities measured by Alice’s analyzer and Bob’s analyzer respectively. Equation (4.6) is valid where there is no eavesdropping. In terms of the detected mode operators given by equations (4.2) - (4.5), this correlation function can be rewritten as

$$E(\theta_1, \theta_2) = \frac{\langle (c_+^t c_+ - c_-^t c_-)(d_+^t d_+ - d_-^t d_-) \rangle}{\langle (c_+^t c_+ + c_-^t c_-)(d_+^t d_+ + d_-^t d_-) \rangle}, \hspace{1cm} (4.7)$$

where $: :$ denotes normal order. This correlation function can be evaluated for the state in (4.1),

$$E(\theta_1, \theta_2) = \cos 2(\theta_1 - \theta_2). \hspace{1cm} (4.8)$$

Using this result, one may estimate Bell’s quantity

$$S = |E(\theta_1, \theta_2) - E(\theta_1, \theta_2')| + |E(\theta_1', \theta_2') + E(\theta_1', \theta_2)|. \hspace{1cm} (4.9)$$
Choosing
\[ \theta = \theta_1 - \theta_2 = \theta'_1 - \theta_2 = \theta'_1 - \theta'_2 = \frac{1}{3}(\theta_1 - \theta'_2), \]
we obtain
\[ S = 3 \cos 2\theta - \cos 6\theta. \] (4.10)
Consider \( \theta_1 = 0, \theta'_1 = \pi/4 \) for Alice's analyzer and \( \theta_2 = \pi/8, \theta'_2 = 3\pi/8 \) for Bob's analyzer. The we have \( S = 2\sqrt{2} \). It is clear that this violates Bell's inequality \(|S| < 2\). This result has also been obtained in [32].

When Eve's eavesdropping occurs (of course in the arm towards Bob only, which is different from the conventional method where both EPR arms are attacked), by such means as measuring and substituting photons, the correlation function then has the form (see Appendix A at the end of this chapter):

\[ E(\theta_1, \theta_2) = \int \rho(\theta_e) \langle \Psi_{ae} \mid (c^\dagger_+ c^\dagger_- - c^\dagger_- c^\dagger_+) \mid \Phi_{ae}(\theta_e) \rangle \langle \Phi_{eb}(\theta_e) \mid (d^\dagger_+ d^\dagger_- - d^\dagger_- d^\dagger_+) \mid \Psi_{eb} \rangle d\theta_e \]
\[ \int \rho(\theta_e) \langle \Psi_{ae} \mid (c^\dagger_+ c^\dagger_- + c^\dagger_- c^\dagger_+) \mid \Phi_{ae}(\theta_e) \rangle \langle \Phi_{eb}(\theta_e) \mid (d^\dagger_+ d^\dagger_- + d^\dagger_- d^\dagger_+) \mid \Psi_{eb} \rangle d\theta_e, \] (4.11)

where
\[ |\Phi_{ae}(\theta_e)\rangle = (s^\dagger_+ s_+ - s^\dagger_- s_-) |\Psi_{ae}\rangle \]
\[ |\Phi_{eb}(\theta_e)\rangle = (s^\dagger_+ s_+ - s^\dagger_- s_-) |\Psi_{eb}\rangle \]
with
\[ s_+ = e_+ \cos \theta_e + e_- \sin \theta_e, \]
\[ s_- = -e_+ \sin \theta_e + e_- \cos \theta_e. \]

All operators in (4.11) are in normal order. \( |\Psi_{xy}\rangle \) is an entangled two-photon state corresponding to modes \( x \) and \( y \) in the case that Eve is present. \( e_\pm \) denotes Eve's modes. The angle \( \theta_e \) in Eve's apparatus is distributed according to some density \( \rho(\theta_e) \). (4.11) can be expressed as an explicit form,

\[ E(\theta_1, \theta_2) = \int \rho(\theta_e) \cos 2(\theta_1 - \theta_e) \cos 2(\theta_2 - \theta_e) d\theta_e. \] (4.12)
The eavesdropping is equivalent to inducing an EPR local reality on the EPR arm towards Bob. Substituting (4.12) into (4.9) and considering $\theta_1 = 0, \theta'_1 = \pi/4$ for Alice's analyzer and $\theta_2 = \pi/8, \theta'_2 = 3\pi/8$ for Bob's analyzer, we obtain $S = \sqrt{2}$. Clearly, this does not violate Bell's inequality. For comparison, in figure 4.1, we plot $S$ as a function of $\theta$ both in the presence of eavesdropping, (4.8), and in the absence of eavesdropping.

![Figure 4.1](image)

**Figure 4.1** Bell's $S$ quantity is plotted as a function of $\theta$. The solid-curve plots the case free of eavesdropping. The dashed-line (with an intercept of about 1.4) represents the case of eavesdropping.

Following Ekert's method [13], Alice and Bob choose orientations of their analyzers and knowing that some of them will be identical and some of them will be different. The results from the measurements with different orientations are used to calculate the $S$ value, for which the calculation of a typical example was illustrated above. If the signal is not directly or indirectly disturbed, namely violation of Bell's inequality is observed, the results from the measurements using the same orientation can be used as a secret key. A suitable choice of the directions of the analyzers is: $\theta_1 = 0, \pi/4, \pi/8; \theta_2 = \pi/8, 3\pi/8, \pi/4$. 
4.3 SPIN-$\frac{1}{2}$-PARTICLE-BASED SYSTEM

In the following, we show that the system based on spin-$\frac{1}{2}$ particles has a similar feature. Suppose that the direction of Alice's analyzer is represented by a unit vector $\vec{a}$ and the direction of Bob's analyzer is a unit vector $\vec{b}$. A source controlled by Alice produces a pair of spin-$\frac{1}{2}$ particles $\alpha$ and $\beta$, which have an opposite spin direction. Particle $\alpha$ which is kept by Alice has spin described by the spin matrix $\sigma(\alpha)$ and particle $\beta$ which travels toward Bob has spin described by $\sigma(\beta)$.

The quantum-mechanical correlation function, in the case of the singlet state, is given by

$$E(\vec{a}, \vec{b}) = \langle \psi_{\alpha\beta} | \vec{a} \cdot \vec{\sigma}(\alpha) \otimes \vec{\sigma}(\beta) \cdot \vec{b} | \psi_{\alpha\beta} \rangle = -\vec{a} \cdot \vec{b}. \quad (4.13)$$

where the singlet state $|\psi_{\alpha\beta}\rangle = \frac{1}{\sqrt{2}}(u_{\alpha}^{+}u_{\beta}^{-} - u_{\alpha}^{-}u_{\beta}^{+})$. $u_{\alpha}^{+}$ and $u_{\alpha}^{-}$ are eigenvectors corresponding to the eigenvalues $+1$ and $-1$, respectively, of the Pauli matrix $\sigma_{z}(\alpha)$ that represents the third component of the spin angular momentum for $\alpha$. $u_{\beta}^{+}$ and $u_{\beta}^{-}$ are the eigenvectors corresponding to the eigenvalues $+1$ and $-1$ for the Pauli matrix $\sigma_{z}(\beta)$ for $\beta$. Consider two orthogonal unit vectors $\vec{a}$ and $\vec{a}'$, associated with particle $\alpha$ and two orthogonal unit vectors $\vec{b}$ and $\vec{b}'$, associated with particle $\beta$. According to (4.13), using $0$ and $\frac{1}{2}\pi$ for $\vec{a}$ and $\vec{a}'$ and $\frac{1}{4}\pi$ and $\frac{3}{4}\pi$ for $\vec{b}$ and $\vec{b}'$, it is easy to show that

$$S = |E(\vec{a}, \vec{b}) - E(\vec{a}, \vec{b}')| + |E(\vec{a}', \vec{b}') + E(\vec{a}', \vec{b})| = 2\sqrt{2}. \quad (4.14)$$

When Eve is present on the EPR arm towards Bob, the correlation function is given by

$$E(\vec{a}, \vec{b}) = \int \rho(\vec{e})d\vec{e}\langle \psi_{ae} | \vec{a} \cdot \vec{\sigma}(\alpha) \otimes \vec{\sigma}(\epsilon) \cdot \vec{e} | \psi_{ae} \rangle \langle \psi_{\epsilon\beta} | \vec{\epsilon} \otimes \vec{\sigma}(\beta) \cdot \vec{b} | \psi_{\epsilon\beta} \rangle$$
$$= \int \rho(\vec{e})d\vec{e} \langle \vec{a} \cdot \vec{e} \rangle \langle \vec{b} \cdot \vec{e} \rangle, \quad (4.15)$$

\[ \text{where } \rho(\vec{e}) \text{ is the density matrix of Eve.} \]
where \( \vec{e} \) denotes the unit vector associated with particle \( \varepsilon \) sent by Eve; \( \vec{\sigma}(\varepsilon) \) denotes the Pauli matrix for \( \varepsilon \); the normalized probability \( \rho(\vec{e}) \) describes the eavesdropper's strategy. Using the same parameters as those used in (4.14), in (4.15) we obtain \( S = \sqrt{2} \), which clearly does not violate Bell's inequality. This result suggests that the spin-\( \frac{1}{2} \)-particle-based system using one EPR arm is also secure.

In conclusion, we have shown the correctness of Ekert's protocol. The agreement between Ekert's calculation and our calculation is that eavesdropping on the EPR arm towards Bob leads to no violation of Bell's inequality therefore revealing any attempt at eavesdropping.

Appendix A

The correlation of random variables \( A \) and \( B \) is defined by

\[
C(A, B) = \frac{1}{M} \langle AB \rangle,
\]

provided \( \langle A \rangle = \langle B \rangle = 0 \), where \( M = ||A|| \cdot ||B|| \). Suppose that \( E \) represents a random variable due to Eve and \( f \) denotes the probability density function of \( E \), then the correlation function of \( A \) and \( B \) may be derived as follows:

\[
C(A, B) = \frac{1}{M} \int \int ab f_{AB}(a, b) dadb
\]

\[
= \frac{1}{M} \int \int ab \int f_E(e) f_{AB|E}(a, b|e) dadbde
\]

\[
= \frac{1}{M} \int f_E(e) \int \int ab f_{AB|E}(a, b|e) dadbde,
\]

where \( f_{AB} \) and \( f_{AB|E} \) are the joint probability density function of \( A \) and \( B \), and the conditional joint probability density function given \( E \) respectively. If \( A \) and
$B$ are independent when $E$ is given, then

$$C(A, B) = \frac{1}{M} \int f_E(e) \left[ \int a f_{A|E}(a|e) da \int b f_{B|E}(b|e) db \right] de$$

(4.18)
In this chapter, we investigate quantum cryptographic protocols which could be suitable for conference key distribution systems. The information theoretical limits are shown to describe quantum-cryptographically protected multi-user optical communication channels. An estimation of the eavesdropping via "intercept/resend" for each quantum system is given. It is shown that the information and correlation formalism reveals such attacks.

The chapter is arranged as follows: Section 5.1 introduces our conference key distribution models; Section 5.2 is devoted to studying the information theory on the conference key distribution protocols; Section 5.3 presents the theory of the correlation function. In the final section, we discuss some other the conference key distribution systems and summarize our work. Part of contents of this chapter has been published in Proceeding of International Symposium on Information Theory & Its Applications. [25]

Before we start, it should be made clear that there are some fundamental problems for practical uses of our quantum conference key protocols. These problems will be summarized in the conclusion of this chapter. We also like to thank one of thesis referees pointed out some of these problems.
5.1 CONFERENCE KEY DISTRIBUTION PROTOCOLS

Quantum cryptographic communication based on the BB protocol involves two users, who share no secret information, together with an adversary Eve who eavesdrops on their communications. A multi-user cryptosystem involves complicated cryptographic communication, including quantum key distribution and system configurations, since a quantum cryptographic channel is based on two-user communication. In figures 5.1 (a) and (b), we propose two quantum conference key distribution systems for N legitimate users $U_0, U_1, U_2, ..., U_{N-1}$. Figure 5.1 (a) describes a fan-shaped configuration; and (b) presents a series configuration. Many other configurations can be constructed based on these.

![Figure 5.1 A schematic diagram of the quantum conference key distribution cryptosystems with N legitimate users. (a) shows a fan-shaped configuration; (b) shows a series configuration.](image)

In the case of the fan-shaped configuration, we consider two ways for the key construction between legitimate users. For method one, or type $F_1$, we consider a quantum protocol similar to the BB protocol, where as principal user or chair, $U_0$ sends a random sequence of single-photon pulses based on either $B_1$ or $B_2$ (with a 50-50 chance for each basis) to $U_1, U_2, U_3, ..., U_{N-1}$ respectively. The photon pulse for every channel, at any instant time should be polarized to the same direction. Subsequently, receivers measure each photon pulse using the measuring bases, $B_1$ or $B_2$, which are chosen randomly and independently. In contrast to the BB protocol in the two-user situation, in the public discussion $U_0$ has to be told which basis has been chosen for each photon pulse by every other
user, then she tells them which measuring basis is correct. The correct basis is
the basis used correctly by all the users in the relevant measurements. They then
agree to discard measurements which used an incorrect basis and those were lost
in the transmissions. The remaining photon pulses, which have been correctly
measured, are used as a shared key distribution in future secure communications.

In the above scenario, if a photon state (sent to all other users by $U_0$), say $|\alpha\rangle_{U_0}$,
survives all measurements via legitimate users, it is used for key distribution.
Note that all users receive a photon pulse (state) possessing the same polarization,
ence, for the sake of simplicity, we denote it by $|\alpha\rangle_{U_0}$. We assume that there is a
common operator, $\hat{U}$, responsible for the measurement of $|\alpha\rangle_{U_0}$, where $|\alpha\rangle_{U_0}$ is an
eigenvector of $\hat{U}$. Then all the elements in the final key distribution are obtained
in terms of the measurement:

$$\hat{U}|\alpha\rangle_{U_0} = \alpha|\alpha\rangle_{U_0},$$

(5.1)

where $\alpha \in \{0, 1\}$, $|\alpha\rangle_{U_0} \in \{|\rightarrow\rangle, |\uparrow\rangle, |\downarrow\rangle, |\swarrow\rangle, |\nwarrow\rangle\}$, and $\hat{U} \in \{\hat{O}_{B_1}, \hat{O}_{B_2}\}$. More explicitly,

$$\hat{U} = \begin{cases} 
\hat{O}_{B_1}, & \text{when } \hat{U}_0 = \hat{U}_1 = ... \hat{U}_{N-1} = \hat{O}_{B_1}, \\
\hat{O}_{B_2}, & \text{when } \hat{U}_0 = \hat{U}_1 = ... \hat{U}_{N-1} = \hat{O}_{B_2}.
\end{cases}$$

(5.2)

$\hat{U}_i$ is obtained by choosing $\hat{O}_{B_1}$ and $\hat{O}_{B_2}$ randomly and independently,

$$\hat{U}_i = \text{Rand}(\hat{O}_{B_1}, \hat{O}_{B_2}), \quad (i = 0, 1, 2, ..., N - 1),$$

(5.3)

where Rand, obtained using a random number generator, is either $\hat{O}_{B_1}$ or $\hat{O}_{B_2}$.

The probability that a single-photon pulse survives the measurements is $2^{-(N-1)}$.
This suggests that the probability is a decreasing function of the number of users.

For method two, or type $F_2$ (also Fig. 5.1 (a)), a conference key distribution
is established by utilizing a combined channel. As chair, $U_0$ first generates a
conference key distribution herself, using her own random number generator. In
order to send the conference key to other legitimate users, she has to establish private keys with all other users through quantum channels. Hence based on the BB protocol private quantum key communications are established for each pair of users, \( U_0 \leftrightarrow U_1, U_0 \leftrightarrow U_2, U_0 \leftrightarrow U_3, \ldots \). We denote the keys as \( k_{U_0 U_1}, k_{U_0 U_2}, k_{U_0 U_3}, \ldots \). Obviously, \( U_0 \) knows all the information about the key distributions. In order to send the conference key distribution, say \( K_{\text{conf}} \), to another user, say \( U_i \), \( K_{\text{conf}} \) must have the same size as the local private key distribution \( k_{U_0 U_i} \) between \( U_0 \) and \( U_i \). After all the private keys have been established, the conference key can be sent to all legitimate users through a classical channel. The information sent to \( U_i \) through the classical channel is a Boolean addition between these keys,

\[
C_{0i} = K_{\text{conf}} \oplus k_{U_0 U_i}, \quad (5.4)
\]

which releases no information to an eavesdropper. The conference key can be extracted by \( U_i \) by

\[
K_{\text{conf}} = C_{0i} \oplus k_{U_0 U_i}. \quad (5.5)
\]

For the series configuration, figure 5.1 (b), we also consider two ways to establish a conference key distribution. The first or type \( S_1 \), is similar to type \( F_1 \), \( U_0 \) the principal user or chair sends a random sequence of information to \( U_1 \) using the BB protocol; after measuring each photon pulse as Bob, \( U_1 \) then reproduces it and sends it to \( U_2 \) (after all bits have been transmitted by \( U_0 \)); \( U_2 \) follows the same method to pass the information to \( U_3 \); this process is continued from \( U_i \) to \( U_{i+1} \) until the final user receives the information. Note here that by "reproduce" we mean that \( U_i \) produces a similar (new) photon pulse that has the same polarization to the one he has measured (including incorrect measurements arising due to the uncertainty principle). Obviously, only part of the instances which have been measured using a correct operator can be "reproduced"; the rest are incorrect (all incorrect instances can be discarded after a public discussion). In the public discussion all users (except the chair) announced publicly which operator
was used for each measurement, thus they are aware of any photon pulse which has survived (with the help of "regeneration") after the final user's measurement. Thus they are able to determine which pulses will be used in the conference key distribution which will be shared by all legitimate users. Since losses caused by each user's measurement, the number of users is limited. This method is not practical if a number of users are involved.

In the second case of series configuration, type $S_2$, which is similar to type $F_2$, $U_0$ prepares a conference key distribution which will be sent using the private quantum keys established between all pairs, $U_0 \leftrightarrow U_1$, $U_1 \leftrightarrow U_2$, $U_2 \leftrightarrow U_3$, ..., based on the BB protocol. The conference key distribution chosen by the chair is sequentially propagated from $U_0$ to other legitimate users, one after the other, via Boolean addition through a classical channel. Each user plays a role as a repeater,

$$U_0 \rightarrow U_1 : \quad C_{01} = K_{conf} \oplus k_{U_0U_1}, \quad K_{conf} = C_{01} \oplus k_{U_0U_1};$$
$$U_1 \rightarrow U_2 : \quad C_{12} = K_{conf} \oplus k_{U_1U_2}, \quad K_{conf} = C_{12} \oplus k_{U_1U_2};$$
$$U_2 \rightarrow U_3 : \quad C_{23} = K_{conf} \oplus k_{U_2U_3}, \quad K_{conf} = C_{23} \oplus k_{U_2U_3};$$

......

Eavesdropping (say, intercept/resend) on any branch of the quantum channel can be detected since the eavesdropper has to randomly choose the basis in an attack so that some information must be randomized (which leads to the possibility that the legitimate users disagree). The multi-user situation provides more opportunities for eavesdroppers, this case is thus more complicated. For the fan-shaped configuration, $F_1$, an eavesdropping attack can be detected only by a pair of users (including the chair) whose communication has been attacked (we exclude a grouped attack, which will be discussed later). For the series configuration, $S_1$, a single eavesdropping will affect later communications for the rest of users.
Once an attack has been detected, the key establishment has to be restarted after all eavesdroppers have been removed. An eavesdropper can only avoid being detected, if she/he manages to choose the correct measuring basis as that of the targeted legitimate users. This is not possible unless she gets access to at least one of the random number generators used by the legitimate users.

For configurations $F_2$ and $S_2$, before sending the conference key distribution, $U_0$ must make sure all private keys are secure. To do this, user $U_i$ sends $U_0$ a string message encrypted by the private key $k_{U_0U_i}$, through a classical channel. After $U_0$ has decrypted it, also using $k_{U_0U_i}$, $U_i$ speaks publicly about the content of the message. If $U_0$ finds the message she has measured is not identical to that of $U_i$, she is then aware that the private key is not secure and the eavesdropper must be removed. The same procedure must be repeated with all users.

We should also point out potential attacks of grouped eavesdroppers who communicate each other. Our main concern is focused on type $F_1$. When the number of legitimate users is sufficiently large, eavesdroppers can extract by dividing the channels connecting $U_0$ and other users into two groups; group one is measured by using $\hat{O}_{B_1}$ and group two is measured by using $\hat{O}_{B_2}$. For a physical pulse, one of the measuring operators must have been used incorrectly and will thus lead to uncertain results in those measurements. Meanwhile, the measurements in the other group definitely provide the correct result. If a number of eavesdroppers are involved, they can immediately discovered which measurement is correct without any information about encoding bases! Notice that this method can only be valid when the number of legitimate users is sufficiently large. Three or four legitimate users are not enough to provide eavesdroppers with sufficient chances to eavesdrop (later, we will have more discussion using channel information theory). The other three schemes remain secure against any multi-eavesdropper attack.
All conference key distribution protocols in this work are based on the BB protocol. To simplify our analysis in the rest of this work, we define two conditions:

*Condition ζ₁*: $U_0$ sends $U_i$ a random sequential photon pulse based on one of four canonical photon states related to bases $B_1$ or $B_2$. We assume that the probability of each state is equal. To be consistent, there is also equal probability for "0" and "1" to occur. $U_i$ measures the photon state by choosing a measuring operator, $\hat{O}_{B_1}$ or $\hat{O}_{B_2}$ randomly and independently, so that the probability of each operator being chosen is $1/2$. However, $U_0$ and $U_i$ do not carry out any public discussion about which measuring basis (operator) has been used. Note that if the basis used by $U_i$ was wrong, $U_i$ has probability $1/2$ of obtaining "0" or "1".

*Condition ζ₂*: Initially, the same as condition ζ₁. However, $U_0$ and $U_i$, now discuss publicly which basis is correct for each measurement and agree to discard all instances in which incorrect bases have been used by $U_i$ in the measurements.

For example, for a two-user system, the mapping for sent/received signal bits corresponding to conditions ζ₁ and ζ₂ are shown in figure 5.2.

We now assume that all eavesdroppers use the "intercept/resend" method and perform their measurements using methods similar to those of a legitimate user $U_i$, i.e. randomly choosing measuring basis (probability $1/2$ for each basis).

### 5.2 INFORMATION THEORY OF MULTIUSER CRYPTOSYSTEMS

Information theory can be used to estimate the merit of quantum channels. Here, we investigate how eavesdropping affects the information flow, and how much information Eve can obtain from eavesdropping.
5.2.1 Information theory in Quantum Channels

Information theory for the BB protocol

We now develop the information formalism for the multiuser system of quantum cryptography, based on information theory [33].

We first consider a two-user quantum cryptosystem based on the BB protocol. Assume that there are two users, $A$ and $B$, the average mutual information can be defined as:

$$I(\hat{B}; \hat{A}) = H(\hat{B}) - H(\hat{B}|\hat{A}),$$

where

$$H(\hat{B}) = - \sum_{i=1}^{2} P(b_i) \log_2 P(b_i),$$
\[ H(\hat{B}|\hat{A}) = -\sum_{i=1}^{2} \sum_{j=1}^{2} P(a_i)P(b_j|a_i) \log_2 P(b_j|a_i), \]

the lower-case characters represent the eigenvalues of the corresponding operators. \( \hat{A} (\hat{B}) \) is a quantum-mechanical operator denoting a measurement by \( A (B) \). \( \hat{A}, \hat{B} \in \{\hat{O}_{B_1}, \hat{O}_{B_2}\} \). Using quantum-mechanical states to represent the condition probabilities, we have \( P(b_j|a_i) \equiv |\langle a_i|b_j \rangle|^2 \).

Under the BB protocol, channel information based on (5.6) becomes

\[ I(\hat{B}; \hat{A}) = 1 + \frac{1}{2} \sum_{i=1}^{2} \sum_{j=1}^{2} P(b_j|a_i) \log_2 P(b_j|a_i) \text{ (bits).} \]  

(5.7)

This quantity varies between 0 and 1, where 1 corresponds to full channel information; 0 corresponds to zero channel information. Assuming that \( a_i \) and \( b_j \) have binary values either 0 or 1. The information for condition \( \zeta_1 \) can be obtained from:

\[ I(\hat{B}; \hat{A}) = \frac{3}{4} \log_2 3 - 1. \]  

(5.8)

In the presence of Eve, the information is then given by

\[ I_E(\hat{B}; \hat{A}) = 1 + \frac{1}{2} \sum_{i=1}^{2} \sum_{j=1}^{2} \left[ \sum_{k=1}^{2} p(b_j|\epsilon_k)p(\epsilon_k|a_i) \right] \log_2 \left[ \sum_{k=1}^{2} p(b_j|\epsilon_k)p(\epsilon_k|a_i) \right]. \]  

(5.9)

Under condition \( \zeta_1 \) we obtain the mutual information when Eve is present,

\[ I_E(\hat{B}; \hat{A}) = \frac{1}{8} (3 \log_2 3 + 5 \log_2 5) - 2. \]  

(5.10)

Following Barnett et al. [34], we introduce a dimensionless parameter \( \xi_{AB} \) defined by

\[ \xi_{AB} = \frac{I_E(\hat{B}; \hat{A}) - I(\hat{B}; \hat{A})}{I_{\text{max}}(\hat{B}; \hat{A})}, \]  

(5.11)

where the maximum mutual information \( I_{\text{max}} \) is 1 in above cases and \(-1 \leq \xi_{AB} \leq 1\). \( \xi_{AB} < 0 \) indicates the eavesdropper has caused a reduction of information in the quantum channel between \( A \) and \( B \) and \( \xi_{AB} > 0 \) indicates an increase of
information. $\xi_{AB} = 0$ represents the absence of eavesdropping, or, the eavesdropping is undetectable which occurs only in the case where the eavesdropper chose identical measuring bases to $B$. Fortunately, the probability of the eavesdropper having so chosen is almost zero when the size of the information string is large. Using (5.8) and (5.10) we obtain: $\xi_{AB} = -0.1431$, as the evidence of eavesdropping.

For condition $\zeta_2$, in the absence of eavesdropping, from (5.7) we obtain the mutual information $I(\hat{B}; \hat{A}) = 1$ if the measurement via $B$ is perfect; in the presence of eavesdropping, the channel information is $I_E(\hat{B}, \hat{A}) = \frac{3}{4} \log_2 3 - 1$. Using (5.11), we obtain $\xi_{AB} = -0.8$, also showing an incidence of eavesdropping.

How much information can Eve obtain from her eavesdropping? Our calculation shows $I(\hat{A}, \hat{E}) = \frac{3}{4} \log_2 3 - 1 \approx 0.12$, agreeing with (5.8). In comparison, the value is 1 for a perfect detection by Bob; so Eve virtually achieves nothing. Moreover, her detection has led to a significant change of the information flow, as we showed previously.

**Channel information for type $F_1$**

Next, we consider the conference key distribution systems. For type $F_1$, we assume that the discrete quantum channels can be treated as an integrated channel. This is valid only if $U_0$ sends an identical photon signal to all other users. In the presence of a number, $N_E$, of eavesdroppers, if each invaded quantum channel has only one attacker who attacks only once and the eavesdroppers do not communicate with each other, using condition $\zeta_2$, the channel information can be expressed as

$$I_{F_1} = I(\hat{X}; \hat{U}_0) = W + \frac{1}{2} \sum_{i=0}^{2^W} \sum_{j=1}^{2^W} P(x_j | u_0 = i) \log_2 P(x_j | u_0 = i),$$  \hspace{1cm} (5.12)
where $\hat{X} = (\hat{U}_1, \hat{U}_2, \cdots, \hat{U}_{N-1})$; the eigenvalues are $x = (u_1, u_2, \cdots, u_{N-1})$, with $u_j = "0"$ or "1"; $x_j$ denotes the $j$th state of $x$;

$$W = \begin{cases} 
N_E + 1, & \text{if } N - N_E > 1 \text{ and } N_E > 0 \\
N_E, & \text{if } N - N_E = 1 \text{ and } N_E > 0 \\
1 & \text{if } N_E = 0
\end{cases}$$

and

$$P(x_j|u_0 = i) = P(u_1, u_2, \ldots, u_{N-1}|u_0 = i)$$
\begin{align*}
&= P(u_1|u_0 = i)P(u_2|u_0 = i) \cdots P(u_{N-1}|u_0 = i),
\end{align*}
(5.13)

which is the conditional probability given $N_E$ eavesdropping attacks.

For example, if there are four users, $\hat{X} = (\hat{U}_1, \hat{U}_2, \hat{U}_3)$; the eavesdropper only attacks the quantum channel between $U_0$ and $U_1$; $x$ has four states $x_1 = (0, 0, 0)$, $x_2 = (1, 0, 0)$, $x_3 = (0, 1, 1)$, $x_4 = (1, 1, 1)$; then we can use (5.13) to calculate the conditional probability, for instance

$$P(x_1|u_0 = 0) = P(u_1 = 0, u_2 = 0, u_3 = 0|u_0 = 0)$$
\begin{align*}
&= P(u_1 = 0|u_0 = 0)P(u_2 = 0|u_0 = 0)P(u_3 = 0|u_0 = 0) \\
&= 3/4 \times 1 \times 1 = 3/4,
\end{align*}

and so on. Our discussion is valid only if the following assumption is true: when a user chooses a wrong basis he has probability $1/2$ of receiving "0" or "1", which is consistent with condition $\zeta_2$. In the absence of eavesdropping, (5.12) gives $I_{F_1} = 1$.

The information loss due to eavesdropping is an increasing function of the number of eavesdroppers. Consistently, the channel information expressed by (5.12) is a decreasing function of the number of eavesdroppers.
CHAPTER 5 QUANTUM CONFERENCE KEY DISTRIBUTION SYSTEMS

Figure 5.3 The mapping for grouped eavesdropping. Failure means that eavesdroppers cannot identify the information, as they have to obtain identical bits in measurements based on an incorrect basis. We have assumed that if grouped eavesdroppers obtain different bits in measurements under the same basis, they know they have used an incorrect basis.

As an example, we calculate the information of four legitimate users as a function of $N_E$,

$$N_E = 1, \quad I_{F_1} = 0.824;$$
$$N_E = 2, \quad I_{F_1} = 0.648;$$
$$N_E = 3, \quad I_{F_1} = 0.0715.$$

The result here presented is obtained using condition $\zeta_2$ and assuming the eavesdroppers do not add in any of their own information.

If the eavesdroppers communicate with each other, the security of $F_1$ will be seriously threatened, especially when there are many users. The strategy of grouped eavesdroppers is as follows:

If only three users including the chair (i.e. two quantum channels) involve the conference-key protocol, then consistently two eavesdroppers may also be involved the eavesdropping. For implementing a grouped attack, the eavesdroppers divide themselves into two groups, and each thus has one eavesdropper and employs a different measuring basis ($B_1$ or $B_2$). In an implementation of the $F_1$ protocol, the chair sends each her partner a bit (say “1”) which is encoded using $B_1$ or $B_2$.
chosen at random. The eavesdroppers intercept and measure the corresponding bit. One of groups must obtain a correct measurement, i.e. "1" is obtained, because the correct basis is used. The other group must obtain an uncertain result ("1" or "0"), since the incorrect basis is used. If the second group obtain "1" (hence both groups have "1"), the eavesdroppers will be aware that the chair has sent "1" and thus be successful. Although, in this case, they are successful to identify the correct bit, they have no idea about the basis employed by the chair. If the second group obtains "0" (hence each group has a different result), they will not be able to know which one is correct bit and thus fail. Note that grouped two eavesdroppers can obtain correct bit information, but they cannot regenerate a similar bit and resend it because of lack of the corresponding basis information. This situation will be changed if more users and thus more eavesdroppers involve a grouped attack.

A system with four channels may be eavesdropped by four eavesdroppers. Similarly to the above example, eavesdroppers can divide themselves into two groups, two for each group, and each group uses a different measuring basis. Each eavesdropper attacks one channel. In an implementation of the $F_1$ protocol, the chair sends a bit "1" based on the secret, random selected basis $B_1$. In a subsequent grouped attack, both eavesdroppers in the group using $B_1$ will definitely obtain "1" and those in the other group using $B_2$ will obtain an uncertain result ("1" or "0"). If in the second group one eavesdropper obtains "1" and the other one obtains "0", they are then aware that the correct answer is "1" and the basis is $B_1$, because the result in the second group indicates uncertainty which suggests that the basis used in the second group is incorrect. If both eavesdroppers in the second group obtain "1", they still know that the correct result is "1", however they cannot determine the basis. If both eavesdroppers in the second group obtain "0", they will even not be able to determine the correct bit and then fail.
If more legitimate users involve $F_1$ conference key protocol, grouped eavesdroppers will have a better chance. In the following calculation, we will know how much information grouped eavesdropping can achieve. For simplicity, we consider an eavesdropping to be successful if the eavesdroppers obtain a correct bit, and ignore whether they can determine the corresponding basis information.

Assume that there are $2M$ eavesdroppers, say $E_1, E_2, \cdots, E_{2M-1}, E_{2M}$, who are divided into two groups $\{E_1, \cdots, E_M\}$ and $\{E_{M+1}, \cdots, E_{2M}\}$, then the events sent by chair are "$a_1 = 0$" and "$a_2 = 1$" and the events received by eavesdroppers (after communicating each other) are $b_1 = "$0", $b_2 = "$failure" and $b_3 = "$1", where "failure" means that eavesdroppers cannot determine the bit (see figure 5.3). The probabilities concerning the measurement of grouped eavesdroppers are given by

$$p(b_1|a_1) = 1 - 2/2^M,$$
$$p(b_2|a_1) = 1/2^M,$$
$$p(b_3|a_1) = 0,$$
$$p(b_1|a_2) = 0,$$
$$p(b_2|a_2) = 1/2^M,$$
$$p(b_3|a_2) = 1 - 2/2^M,$$
$$P(b_1) = (1 - 2/2^M)/2,$$
$$p(b_2) = 1/2^M,$$
$$p(b_3) = (1 - 2/2^M)/2,$$
Figure 5.4 Channel information for grouped eavesdropping plotted as a function of the number of eavesdroppers.

This leads to the following channel information between the chair and eavesdroppers:

\[
I_{Eve}(\hat{X}_E; \hat{U}_0) = -\sum_{i=1}^{3} p(b_i) \log_2 p(b_i) + \sum_{i=1}^{2} \sum_{j=1}^{3} p(b_j|a_i) \log_2 p(b_j|a_i)
\]

\[
= -(1 - 2/2^M) \log_2((1 - 2/2^M)/2) + 1/2^M \log_2(1/2^M)
\]

\[
+ 2(1 - 2/2^M) \log_2(1 - 2/2^M) + 2(2/2^M) \log_2(2/2^M), (5.14)
\]

where \( \hat{X}_E \) represents the set of operators employed by the eavesdroppers. In figure 5.4, we plot \( I_{Eve} \) as a function of \( M \). We see \( I_{Eve} \) is an increasing function in \( M \). When \( M = N/2 = 2 \), i.e. there are four eavesdroppers, the channel information is 0.2. When \( M = N/2 >> 1 \), the channel information is approximately 1 which indicates full information. This is achieved without being told any basis information. Actually, a large number of grouped eavesdroppers can discover basis information employed in the chair's coding, in terms of their grouped measurements. After having full basis information, the eavesdroppers enable to regenerate and thus to resend the signal to corresponding legitimate users. This suggests that we will have \( I_{F_i} = 1 \), namely the eavesdropping cannot be detected.
Channel information for type $S_1$

For type $S_1$, the series configuration, a signal pulse has to be measured and resent by each user in turn reproducing the measurement. In order to study the channel information for the system, we first introduce a transition probability matrix between legitimate users $U$ and $V$, under condition $\zeta_2$,

$$Q_{UV} = \begin{pmatrix} q_{u_0v_0} & q_{u_0v_1} \\ q_{u_1v_0} & q_{u_1v_1} \end{pmatrix}, \quad (5.15)$$

where

$$q_{u_iv_j} = P(v = j|u = i).$$

The subscripts 0 and 1 denote a binary signal.

The transition probability matrix for users $U_0$ and $U_i$ in the series configuration is then

$$Q_{U_0U_i} = Q_{U_0U_0}Q_{U_0U_1}Q_{U_1U_2}Q_{U_2U_3} \cdots Q_{U_{i-1}U_i}. \quad (5.16)$$

The joint probability, in terms of the transition matrix, is given by

$$P(u_i = j, u_0 = k) = P(u_0 = k)q_{u_0h_i,j}, \quad (k, j = 0, 1). \quad (5.17)$$

The mutual information for the quantum channel between $U_0$ and $U_i$ is defined by

$$I(\hat{U}_i; \hat{U}_0) = 1 + \frac{1}{2} \sum_{k,j=0}^1 P(u_i = j|u_0 = k) \log_2 P(u_i = j|u_0 = k). \quad (5.18)$$

Assume that there are $N$ users and $N_E$ eavesdroppers ($N - 1 \geq N_E \geq 0$) and each one quantum channel connecting two neighbouring users has at most one eavesdropper. So $N_E$ quantum channels are attacked. For simplicity, we further assume that the first $N_E$ quantum channels are targeted. The transition probability matrix can then be expressed as

$$Q_{u_0u_{N-1}} = Q_{1}^{N_E} Q_{2}^{N-N_E-1}, \quad (5.19)$$
where $Q_1$ is the transition probability matrix between two neighbouring users whose channel is attacked and $Q_2$ is an ordinary transition probability matrix of two attack-free neighbouring users. After a simple calculation, we find

$$Q_1 = \begin{pmatrix} 3/4 & 1/4 \\ 1/4 & 3/4 \end{pmatrix}, \quad Q_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad (5.20)$$

where we have used condition $\zeta_2$. In terms of (5.15) and (5.17), we find the average mutual information is

$$I_{S_1} = \begin{cases} 1, & (N_E = 0) \\ \frac{1}{N-1} \left[ \sum_{k=1}^{N_E} I(\hat{U}_0; \hat{U}_k) + (N - N_E - 1)I(\hat{U}_0; \hat{U}_E) \right], & (N_E \geq 1) \end{cases} \quad (5.21)$$

where

$$I(\hat{U}_0; \hat{U}_k) = \begin{cases} 1 - \frac{3}{4}(k + 1) + \frac{1}{2^{k+1}} \log_2[(2^k - 1)(2^{k-1})(2^k + 1)(2^{k+1})/2], & (k \leq N_E) \\ 1, & (N_E = 0) \\ I(\hat{U}_0; \hat{U}_{N_E}). & (k > N_E \geq 1) \end{cases}$$

Similarly to the case of type $F_1$, $I_{S_1}$ is a decreasing function of the number of eavesdroppers.

In condition $\zeta_2$, we mentioned that a photon pulse which has been measured using a wrong basis is discarded. Hence only those photon pulses correctly measured are considered in the calculation of (5.12) and (5.21). However if we consider all the information sent by $U_0$ including that discarded afterwards, the general channel information should be reduced by a factor of $1/2^{N-1}$ because only $1/2^{N-1}$ of the total photon pulses contributed to the conference key distribution. This implies that the channel information is a decreasing function in the number of users, $N$.

The channel information is also a decreasing function in the number of eavesdroppers. This indicates that the channels are secure. Furthermore, in contrast to $F_1$, it is immunized against grouped attacks.
5.2.2 Channel Information of Combined Channels

Channel information for type $F_2$

For type $F_2$, a private quantum key distribution for each quantum channel is established after the chair $U_0$ has chosen a conference key distribution. A zero information string containing the Boolean addition of the related private key and the conference key is sent to each other legitimate user through classical channels by the chair. Therefore, the total number of information involves both quantum and classical channels. Suppose that the conference key distribution generated by $U_0$ is one of $K_{U_0,1}, K_{U_0,2}, \ldots K_{U_0,m}$, where $m$ is total permutations for a certain size of string. The conference key distribution received by another user, $U_i$, might not be the original one due to the possibility of attacks by eavesdroppers on the quantum channels: thus we assume it to be one of $K_{U_i,1}, K_{U_i,2}, \ldots K_{U_i,m}$. Hence, the private quantum key distribution obtained by $U_0$ is one of $k_{U_0,1}, k_{U_0,2}, \ldots k_{U_0,m}$; the private quantum key distribution of $U_i$ is one of $k_{U_i,1}, k_{U_i,2}, \ldots k_{U_i,m}$, where each key distribution has the same size as that of the conference key distribution. The channel information of a pair of users $U_{0,*}$ and $U_{i,*}$, for the general case including eavesdropping is given by

$$I(K_{U_i}; K_{U_0}) = \log_2 m + \frac{1}{m} \sum_{* \neq i=1}^{m} P(K_{U_{i,*}|K_{U_0,*}}) \log_2 P(K_{U_{i,*}|K_{U_0,*}}), \quad (5.22)$$

where the conditional probability of $K_{U_{i,*}}$ given by $K_{U_0,*}$ is

$$P(K_{U_{i,*}|K_{U_0,*}}) = \frac{1}{P(K_{U_{0,*}})} \sum_{l=1}^{m} P(K_{U_{i,1}, K_{U_0,*}, K_{U_0,l}})$$

$$= \frac{1}{P(K_{U_{0,*}})} \sum_{l=1}^{m} P(k_{U_{i,1}^{(s,l,i)}}, K_{U_0,*}, k_{U_{0,l}})$$

$$= \sum_{l=1}^{m} P(k_{U_{i,1}^{(s,l,i)}}, k_{U_{0,l}}, K_{U_0,*})P(k_{U_{0,l}}), \quad (5.23)$$
where \( k_{U_{i,t}(s,t,l)} = K_i \oplus k_t \oplus K'_j \) and \( t'(s, t, l) \) is a function of \( s, t, \) and \( l \). If there are no eavesdroppers and all measurements are perfect,

\[
P(K_{U_{j,t}}|K_{U_{i,t}}) = \begin{cases} 
1 & (s = t, \text{ for all } i, j) \\
0 & (s \neq t) 
\end{cases} \quad (5.24)
\]

**Channel information for type \( S_2 \)**

Equation (5.22) can be used to calculate the average channel information for configurations \( F_2 \) and \( S_2 \),

\[
I_{F_2} = \frac{1}{N - 1} \sum_{i=1}^{N-1} I(K_{U_i}; K_{U_0}). \quad (5.25)
\]

However, for the series configuration, type \( S_2 \), the conference key transition probability matrix between \( U_0 \) and \( U_i \) must be given. For any two users, say \( U_i \) and \( U_j \), the transition matrix is

\[
Q_{U_i,U_j} = \left( P(K_{U_{j,t}}|K_{U_{i,t}}) \right)_{m \times m}, \quad (5.26)
\]

where \( s, t = 1, 2, 3, \ldots, m \). Thus the conference key transition probability matrix between \( U_0 \) and \( U_i \) is expressed as

\[
Q_{U_0,U_i} = Q_{U_0,U_1}Q_{U_1,U_2} \cdots Q_{U_{i-1},U_i}. \quad (5.27)
\]

Equation (5.22) can also be used for the channel information for type \( S_2 \).

An advantage of systems of \( F_2 \) and \( S_2 \) is that the information is not a decreasing function in the number of users, \( N \). This is because, for \( F_2 \) and \( S_2 \), the quantum key distribution is established between each pair of users, but not among all users.

Considering eavesdropping, the average channel information for \( F_2 \) and \( S_2 \) can be written as:

\[
I_{F_2} = \frac{1}{N - 1} \left[ (N - N_E - 1) \log_2 m + \sum_{i=1}^{N_E} I_{U_0 U_i} \right] \quad (5.28)
\]
and
\[ I_{S_2} = \frac{1}{N-1} \left[ (N - N_E - 1) I_{U_0 U_{N_E}} + \sum_{i=1}^{N_E} I_{U_0 U_i} \right] \]  (5.29)
respectively. In (5.29) we have assumed the first \( N_E \) channels are attacked. It can be shown that \( I_{F_2} > I_{S_2} \), if \( N - 1 \geq N_E > 0 \).

5.3 CORRELATIONS IN QUANTUM CRYPTOSYSTEMS

5.3.1 Correlation in Quantum Channels

Channel information can be used to examine the resistance of a conference cryptographic system against eavesdropping, as shown previously. However, we find that in some special circumstances the system channel information cannot reflect the correlation between measurements (which might cause a failure in describing a channel which is under an eavesdropping attack and has a perfect negative correlation). As an example of the failure, see figure 5.5, \( A \) sends binary 0 or 1 to \( B \) who then obtains 0 or 1 with probability either \( P = 0 \) or \( P = 1 \). There are two completely different cases: in figure 5.5 (a), \( B \) receives a totally wrong signal; in figure 5.5 (b), \( B \) receives the correct signal. It is easy to calculate that the channel information, for both cases, has the same value, \( I(\hat{B}; \hat{A}) = 1 \). Although these cases are very rare, we consider another way to estimate the merit of the cryptosystem by using correlation function between users.

For two users, \( A \) and \( B \), the correlation function of \( A \) and \( B \) is defined by
\[ C(\hat{A}, \hat{B}) = \frac{\text{cov}(X_{\hat{A}}, X_{\hat{B}})}{\sqrt{\text{var}(X_{\hat{A}}) \text{var}(X_{\hat{B}})}} \]  (5.30)
where random variables \( X_{\hat{A}} \) and \( X_{\hat{B}} \) are 0 when "0" is measured and 1 when "1" is measured. \( \hat{A} \) is the measuring operator used by \( A \) and \( \hat{B} \) is the measuring operator used by \( B \). If the communication is perfect, \( C(\hat{A}, \hat{B}) = 1 \), and \( A \) and \( B \) are then said to be perfectly correlated. If \( C(\hat{A}, \hat{B}) = 0 \), then \( A \) and \( B \) are
Figure 5.5 A communication between $A$ and $B$ using only two photon pulses "0" and "1". (a) shows that $B$ has a probability of zero of receiving the correct signal and a probability of one of receiving an incorrect signal. (b) shows that $B$ has a probability of one of obtaining the correct signal and a probability of zero of receiving an incorrect signal.

uncorrelated. When the communication between $A$ and $B$ completely fails, we have $C(\hat{A}, \hat{B}) = 0$. The value of the correlation function being between 0 and 1 suggests that the results of the measurements are positively correlated. If the sent and received signals are negatively-correlated, then $-1 < C(\hat{A}, \hat{B}) < 0$. In the cases illustrated in figure 5.5, we have $C(\hat{A}, \hat{B}) = 1$ and $-1$, respectively.

If there is no any intruder between $A$ and $B$, whether $B$ receives a correct message depends only on whether $B$ uses the correct basis relative to $A$'s. It is easy to calculated that, under condition $\zeta_1$, $C(\hat{A}, \hat{B}|\zeta_1) = 1/2$, and under condition $\zeta_2$, $C(\hat{A}, \hat{B}|\zeta_2) = 1$. If there is unique intruder $E$ eavesdropping between $A$ and $B$, we find $C(\hat{A}, \hat{B}|\zeta_1) = 1/4$ and $C(\hat{A}, \hat{B}|\zeta_2) = 1/2$. These values suggest that the eavesdropping decreases the correlation of the measurement.

Next, we consider multiuser cases. Assume that $U_0$ is the chair of a conference and is in charge of the conference key communication, then the average correlation
for $N$ users is
\[ C = \frac{1}{N-1} \sum_{i=1}^{N-1} \frac{\text{cor}(X_{\hat{U}_0}, X_{\hat{U}_i})}{\text{var}(X_{\hat{U}_0})\text{var}(X_{\hat{U}_i})^{1/2}}, \] (5.31)

where $\hat{U}_i$ denotes an operator used by another user $U_i$. This formula can be applied to both types $F_1$ and $S_1$. It is easy to show that when eavesdropping is absent, $\tilde{C}$ has the same value as in the two-user case.

In the presence of eavesdropping, for type $F_1$, if each branch of the quantum channel has at most one eavesdropper, we have
\[ \tilde{C} = 1 - \frac{N_E}{2(N-1)}. \] (5.32)

where $N_E$ is the number of eavesdroppers. We found that $0.5 \leq \tilde{C} \leq 1$. Here we have used the condition $\zeta_2$.

For type $S_1$, the series configuration, we have introduced a transition probability matrix, (5.16) and obtained the joint probability, (5.17). The average correlation can be obtained in terms of the transition probability matrix, using (5.31).

If there are $N$ users and $N_E$ eavesdroppers who attack the quantum channels of the first $N_E$ pairs of users, then using (5.20) and condition $\zeta_2$ we obtain the average correlation for type $S_1$ as
\[ \tilde{C} = \frac{1}{N-1} \left[ \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \ldots + \frac{1}{2^{N_E}} + (N - N_E - 1) \frac{1}{2^{N_E}} \right], \quad (N_E > 0). \] (5.33)

If the intruder attacks the quantum channel between $U_0$ and $U_1$ only, $\tilde{C} = 1/2$.

### 5.3.2 Correlation in Combined Channels

Similarly to the case studied previously, private keys have to be established between each pair of users, for both configurations $F_2$ and $S_2$, via quantum channels, in order for the later use in establishing the conference key. To calculate the correlation between the sent and received conference key distribution, we first define
a transition matrix between $U_i$ and $U_j$,

$$Q(U_i, U_j) = (P(K_{U_j,t}|K_{U_i,t}))_{m \times m}.$$  

(5.34)

The joint probability of $U_i$ and $U_j$ is

$$P(K_{U_j,t}, K_{U_i,t}) = P(K_{U_i,t})P(K_{U_j,t}|K_{U_i,t}).$$  

(5.35)

Note that $\{K_{U_i,t}\}$ has $m$ states and $K_{U_i,t}$ and $K_{U_j,t}$ represents the same conference key for any $i$ and $j$, $t = 1, 2, ..., m$.

We also need to introduce two random variables, $X_{U_0}$ and $X_{U_i}$, taking values

$$X_{U_0} = s, \text{ if } K_{U_0,t} \text{ is sent},$$

$$X_{U_i} = s, \text{ if } K_{U_i,t} \text{ is received},$$

where $s = 1, 2, ..., m$.

Hence the correlation between the information received by $U_0$ and $U_i$ can be obtained in terms of the formula:

$$C(X_{U_0}, X_{U_i}) = \frac{\text{cov}(X_{U_0}, X_{U_i})}{[\text{var}(X_{U_0})\text{var}(X_{U_i})]^{1/2}}.$$  

(5.36)

The system correlation is defined as the average correlation over all users, and is the same as (5.31).

### 5.4 DISCUSSION AND CONCLUSION

More general quantum conference key distribution systems can be established in terms of the basic structures studied in previous sections. The most straightforward model is a ring-configuration, as shown in figure 5.6 (a), which can be compared to the series configurations. Our analysis for series configurations is applicable to a ring-configuration. In figure 5.6 (b), a configuration based on a combination of series configurations is shown. Each branch can be treated as a
CHAPTER 5 QUANTUM CONFERENCE KEY DISTRIBUTION SYSTEMS

Figure 5.6 Quantum conference key systems based on fan-shaped and series configurations. The unshaded circle in each diagram represents the chair.

The number of users in each group seems important for types $F_1$ and $S_1$, since as mentioned previously, the channel information is a decreasing function of $N$. In order to increase the information rate with a large number of users, $U_0$ has to increase the size of the information string, this, we believe, will cost communication time. A reasonable $N$ should be chosen considering the physical requirements for a practical system.

The conference key (figure 5.6) is sent to each group by the chair using classical channels and Boolean addition. In the absence of eavesdropping, each group has a group key. The correlation and information of the channels between the groups can be calculated in terms of the method introduced in the previous sections, provided we treat each group as a single user. However, in the presence of eavesdropping, some group key distributions might have been badly hurt, hence the calculation becomes complicated. Under such a situation, the calculation has to rely on users' keys and relevant quantum channels because the case is different from user to user. The security of a conference key distribution is based on each
group key distribution, where since the establishment of group key distributions involves quantum channels, any attack(s) can be detected before the final conference key distribution is sent by the chair. Consequently, a secure conference key distribution can be established, once all eavesdroppers are removed.

In our study, we have ignored noise which might cause errors and thus is an important factor in our conference key protocols. The problem seems quite serious for configurations $F_i$ and $S_i$, since they require an identical signal for each of their measurements. However we would suggest that hashing technique might be an efficient method to resolve this problem, as it has been successfully demonstrated in the BB protocol [6]. In contrast, the noise problem for configurations $F_2$ and $S_2$ is smaller, simply because the conference key is dependent only on the individual quantum channel which can have very small error rates according to the BB protocol experiment [6].

In conclusion, in this chapter we have investigated quantum conference key distribution protocols. The channel information and correlation between users have been studied to demonstrate the merit of our systems against eavesdropping. However, there are some issues on proposed protocols to be pointed out. (1) We have showed that configurations $F_i$ and $S_i$ have a disadvantage in the restriction of the user population. $F_1$ suffers potential failure under grouped attacks. $S_1$ is inefficient when the number of users is large. (2) Configurations $F_2$ and $S_2$ are more secure than $F_1$ and $S_1$. This is because each pair of legitimate users use different quantum bits to transmit their signal. However, since the conference key is transmitted via a classical channel, it is not "quantized".

Despite these problems on the protocols proposed in this chapter, The valuable thing is that the work provides an overview of conference key protocols based on quantum mechanics.
An ordinary optical measurement inevitably damages the signal after the measurement, due to the introduction of quantum noise. However, there is a measurement scheme which does not add any quantum noise to the signal and conserves the physical features of the signal. Thus the original signal is maintained after the measurement. The method is called quantum nondemolition detection (QND). The aim of the QND is to measure an observable of a system, without the act of measurement disturbing the evolution of the observable at later times. The general theory of QND measurement was developed by Caves et al. [35]. A good interpretation of QND measurement was presented by Braginsky, Vorontsov, and Thorne [36]. A number of QND measurement schemes have been proposed. An experimental demonstration of a QND measurement has been done by Levenson, Shelby, Reid, and Walls [37] using four-wave mixing in optical fibres.

In principle, QND schemes could be used in quantum cryptography for both eavesdropping and multiuser cryptographic systems. However, we wish to know how well they will perform. The only work published involving QND measurement in quantum cryptography was presented by Werner and Milburn [19], where they established a theoretical model of eavesdropping for an EPR type of cryptographic system, but obtained a negative outcome.
In this chapter, we will explore applications of QND measurement to two cryptographic systems. First, we investigate a QND attack on a interferometric system outlined by Bennett [10]. Second, we study the system using an optical coupler as presented in Chapter 3.

6.1 BENNETT'S TWO-STATE SYSTEM AND EAVESDROPPING BY QUANTUM NONDEMOLITION DETECTION

Secure key distributions can be generated using optical wave interaction. A good example was given by Bennett [10] who predicted the usefulness of the optical interferometric system to realize secure key distribution using two nonorthogonal quantum states. The measurement in his protocol is based on two non-commuting projection operators. One property of these operators is that if a wrong operator is used, we will obtain a zero eigenvalue, but not the random value we expect to obtain. In this section, we introduce Bennett's method and investigate an eavesdropping strategy using a QND scheme. Our intention is to examine whether the proposed QND measurement can eavesdrop coherent cryptographic signal without being noticed.

6.1.1 Brief review of the protocol utilizing optical interferometry

In 1992, Bennett proposed a quantum cryptographic protocol using two nonorthogonal states. He chose two nonorthogonal states, \(|u_0\rangle\) and \(|u_1\rangle\), and two non-commuting projection operators, \(P_0 = 1 - |u_1\rangle\langle u_1|\) and \(P_1 = 1 - |u_0\rangle\langle u_0|\). \(P_0\) annihilates \(|u_1\rangle\), but yields positive results when applied to \(|u_0\rangle\), and vice versa for \(P_1\).
Figure 6.1 Bennett's model of interferometric quantum key distribution using two nonorthogonal coherent states. The source on the left supplies coherent pulses (wave form W) of intensity greater than one to Alice's half-interferometer, where asymmetric beam splitters, mirrors, and a phase shifter (PSA = 0° or 180°) produce a dim signal pulse (w or, phase shifted, m), followed by a bright reference pulse W. After being sent to Bob through a single mode optical fiber, the pulses enter Bob's half-interferometer, where, depending on whether the sum of Alice and Bob's phase shifts is 0° or 180°, the signal pulse undergoes constructive (wave form 2w) or destructive (wave form nothing) interference with attenuated reference pulse before entering the detector. Arriving after the interference pulse is a bright, twice-delayed, reference pulse (wave form W) which Bob monitors to be certain the reference pulses are not being suppressed. Also not shown are two unused beams leaving the rightmost beam splitter of each half-interferometer in a downward direction.

A practical realization of those measurements was predicted applying two half-interferometers shown in figure 6.1. Beginning at the left of the figure, Alice uses two asymmetric beam splitters to split an initial coherent light into two pulses separated in time: a dim pulse of intensity less than one is followed by a bright reference pulse of intensity greater than one. The dim pulse is the signal pulse whose phase is shifted either 0° or 180° by a phase shift PSA and then delivered to a single mode optical fibre in the interferometer. The phase of the brighter pulse is not shifted, but is delayed by a fixed time Δt. At the receiving end of the apparatus, Bob uses a half-interferometer, similar to Alice's, to split the incoming beams into a dim part and a bright part, in the same ratio as before.
As before the dim part is phase shifted (PSB) by $0^\circ$ and $180^\circ$, while the bright part is delayed by $\Delta t$. The PSB is independent of Alice's phase shifts. Finally, the two parts are made to interfere as they enter a detector.

The wave entering the detector consists of three pulses separated by time $\Delta t$. The first pulse, a very dim pulse which has been attenuated both by Bob and by Alice but delayed by neither, is not considered further. The second pulse, containing important information, is a dim pulse consisting of the superposition of the beam delayed by Alice and attenuated by Bob, and the beam delayed by Bob and attenuated by Alice. Finally, after a delay $\Delta t$ in the superposed pulse, a bright pulse, which has been delayed by both Alice and Bob but attenuated by neither, will arrive at Bob's detector.

The key distribution can be easily established in such a way that, for example, Alice randomly sends red or green flashes (corresponding to $0^\circ$ and $180^\circ$) of intensity less than one, and Bob would publicly report any flashes he saw (but not their colours). A secret key distribution can be constituted, depending on the colours.

Taking into consideration that two non-commuting measuring operators, $P_0$ and $P_1$, are used, the system can be protected against Eve who has a similar apparatus but with her own phase shifter. If Eve uses $P_0$ all green flashes will be annihilated and if Eve uses $P_1$ all red flashes will be annihilated. This will result in approximate half of flashes being empty states. It is not possible to distinguish whether these empty states come from Eve's measurement or the original signal, hence it is not possible for Eve to resend (to substitute for the signal using her fake signal) without causing substantial changes in the signal.

However, because ordinary coherent states with phase shifted at either $0^\circ$ or $180^\circ$ are used in the system, it is possible for Eve to use either a projection operator
or some other method of detection (for example, a homodyne detection, if the phase reference has been ascertained), The detector can be set to suit 0° states for instance, hence all 0° states CAN be identified. Once Eve finds an empty pulse (no projection), she may guess that the bit is the 180° state. However if Alice’s signal contains many empty pulses, Eve will not be able to know whether the zero represent the 180° state or an empty pulse. This is a basic criterion of the protocol. Nevertheless, this criterion implies some sort of certainty which is true only when the two coherent states are either NOISELESS or ORTHOGONAL. In other words, they do not have any overlap. However this assumption is false according to Bennett’s basic nonorthogonal condition which is essential for security. The basic method for Bennett to get rid of the contradiction is that the phase of each useful dim pulse is associated to a bright phase reference pulse. Hence, although we still have the suspicion of projection uncertainty due to the overlap between each pairs of dim states, we presume that Bennett’s projection operators are correct.

In the following analysis, we accordingly use two projection operators and ignore the issues arising from the overlap in Bennett’s system.

Basic mechanism of QND measurement
Figure 6.2 explains how a QND measurement works, where $A$ represents a signal operator and $B$ represents a probe operator which will be measured by a detector. The incident signal $A(t_0)$ will not be damaged after the QND measurement process is completed. The theory of QND measurement has been described in detail by Caves et al. [35]. To understand the basic mechanism of QND measurement, we briefly review the work by Caves et al. Consider an observable $a$, with the corresponding operator $A(t)$ in a Schrödinger picture. If in a sequence of measurements of $a$, the results of each measurement can be predicted precisely, $a$ is then called QND observable. This can be expressed as

$$A(t) = f(A(t_0), t, t_0),$$

where $f$ is an arbitrary function corresponding to the QND measurement, $t_0$ is the initial time and $t$ is the time after an evolution (or a QND measurement) and $A(t)$ is the output signal. In an interaction picture, above the equation can be written as

$$[A_I(t), A_I(t_0)] = 0,$$

where "$I$" labels the interaction picture. This means that $A_I(t)$ and $A_I(t_0)$ have common results in a measurement.

### 6.1.2 QND attack using parametric frequency conversion

Our model of a QND attack is based on a parametric frequency converter [23] and quantum physics. Assume that the signal mode is represented by $a (a^\dagger)$ which is the annihilation (creation) operator of the field; similarly, the probe mode is represented by $p (p^\dagger)$. The Hamiltonian for this system is given by

$$H = \hbar \omega_a a^\dagger + \hbar \omega_p p^\dagger + \hbar \kappa (a^\dagger e^{-i(\omega_a - \omega_p)t} + c.c.),$$

where $c.c.$ denotes a complex conjugate, $\kappa$ denotes coupling constant, and we have assumed that the damping of both the signal and probe fields is small and
negligible. In an interaction picture, the Hamiltonian can be simplified to

$$H_I = \hbar \kappa (a\dagger e^{-i(\omega_s - \omega_p)t} + c.c.).$$

(6.4)

The Heisenberg equations of motion in the interaction picture are

$$\frac{d\bar{a}}{dt} = -i\kappa \bar{p},$$

(6.5)

$$\frac{d\bar{p}}{dt} = -i\kappa \bar{a},$$

(6.6)

here, \(\bar{a} = a\exp(i\omega_s t)\) and \(\bar{p} = p\exp(i\omega_p t)\). The solution is

$$a = a(0) \cos \kappa t - ip(0) \sin \kappa t,$$

(6.7)

$$p = p(0) \cos \kappa t - ia(0) \sin \kappa t.$$  

(6.8)

where \(t\) is interaction time.

Now we consider Bennett's model. Before proceeding, it is necessary to assume that the weak pulse contains real key information and hence to ignore bright pulses which are for phase reference. This is because the changes (due to the QND interaction) in phase and in the intensity of the bright pulses are negligible (this condition holds if \(\kappa t\) is close to \(2k\pi, k = 0, 1, 2, \cdots\)).

We must design a QND attack which conserves the signal phase. The best way to realize this goal in a present system is to set the probe field be a vacuum state. This, in terms of the above solution, leads to conservation of the phase, i.e., \(\theta(t) = \theta(0)\).

After a QND interaction, the signal amplitude (< 1 on the average) is reduced by a factor of \(\cos \kappa t\) with respect to \(\kappa\) and \(t\). This reduction can be made as small as possible by choosing a suitable interaction interval \(t\). However this choice should also made with respect to the sensitivity of the measurement on the probe output. In order to avoid attenuation in the signal, i.e., \(|a| = |a(0)|\), it may be necessary
to use a non-vacuum state for the probe mode, say a coherent state. However, because of the probe field $b(0)$, conservation of the phase no longer exists. This is easily to be found from (6.7)

$$\theta(t) = \theta(0) + \xi[a(0), p(0), \kappa, t].$$

(6.9)

The difficulty here is that $\xi$ is a function subject to the signal field, but also dependent on Eve’s parameters. This makes it impossible for Eve to use a constant phase shifter to adjust the phase change in the QND interaction.

In order to be consistent to the coding strategy and the noise feature of the QND, we further analyze the light field utilizing quadrature phase amplitudes,

$$a_1(t) = \sqrt{\frac{\hbar}{2\omega}}(ae^{i\omega t} + a^\dagger e^{-i\omega t}),$$

(6.10)

$$a_2(t) = \frac{1}{i} \sqrt{\frac{\hbar}{2\omega}}(ae^{i\omega t} - a^\dagger e^{-i\omega t}),$$

(6.11)

$$p_1(t) = \sqrt{\frac{\hbar}{2\omega}}(pe^{i\omega t} + p^\dagger e^{-i\omega t}),$$

(6.12)

$$p_2(t) = \frac{1}{i} \sqrt{\frac{\hbar}{2\omega}}(pe^{i\omega t} - p^\dagger e^{-i\omega t}),$$

(6.13)

with

$$[a_1, a_2] = i\hbar/\omega, \quad [p_1, p_2] = i\hbar/\omega,$$

(6.14)

where $a_1, a_2$ ($p_1, p_2$) are actually operators corresponding to the real and imaginary components of the signal (probe) mode.

Using solutions (6.7) and (6.8), we have

$$a_1(t) = a_1(0) \cos \kappa t + \sqrt{\omega_p/\omega_a} p_2(0) \sin \kappa t,$$

(6.15)

$$a_2(t) = a_2(0) \cos \kappa t - \sqrt{\omega_p/\omega_a} p_1(0) \sin \kappa t,$$

(6.16)

$$p_1(t) = p_1(0) \cos \kappa t + \sqrt{\omega_a/\omega_p} a_2(0) \sin \kappa t,$$

(6.17)

$$p_2(t) = p_2(0) \cos \kappa t - \sqrt{\omega_a/\omega_p} a_1(0) \sin \kappa t,$$

(6.18)
If the probe field is a vacuum state and the signal field is encoded only in the $x$ axis (in accordance with Bennett’s signal arrangement), the solution under averaging is

\[
\langle a_1(t) \rangle = \pm |\langle a_1(0) \rangle| \cos \kappa t, \tag{6.19}
\]
\[
\langle a_2(t) \rangle = 0, \tag{6.20}
\]
\[
\langle p_1(t) \rangle = 0, \tag{6.21}
\]
\[
\langle p_2(t) \rangle = \pm \sqrt{\omega_a/\omega_p} |\langle a_1(0) \rangle| \sin \kappa t, \tag{6.22}
\]

where “+” and “−” correspond to 0° and 180° respectively. Determining $\langle p_2(t) \rangle$ actually leads to the determination of the signal $\langle a_1(t) \rangle$. In fact, it is not hard to find

\[
a_1(t) = \sqrt{\omega_p/\omega_a} [p_2(0)/ \sin \kappa t - p_2(t) \cos \kappa t], \tag{6.23}
\]

The noise induced by the QND device is

\[
\langle \Delta a_1^2(t) \rangle = \langle \Delta a_1^2(0) \rangle \cos^2 \kappa t + \frac{\omega_p}{\omega_a} \langle \Delta p_2^2(0) \rangle \sin^2 \kappa t. \tag{6.24}
\]

If the probe mode is a squeezed state, $\langle \Delta p_2^2(0) \rangle = 0$, then $\langle \Delta a_1^2(t) \rangle \leq \langle \Delta a_1^2(0) \rangle$. Hence the QND measurement does not add any noise to the signal.

If Eve uses a measuring apparatus similar to Bob’s and uses one projection operator only, she can accurately detect half the string of mode $p$. The remaining results must be zero belonging to the mixture of vacuum states and the other half of the signal string. It is impossible for Eve to amplify these attenuated signal modes, due to the lack of coding information of the signal. If the attenuation is negligible, Eve’s attack is partly successful. This means that the eavesdropping may not be revealed. However, since a large fraction of the information on the key is still unknown to Eve, the eavesdropping eventually fails.
6.2 THE QND ATTACK ON THE PROTOCOL USING AN OPTICAL COUPLER

We now apply the same QND scheme to our system studied in Chapter 3, i.e., the system based on an optical coupler. The system differs from Bennett's system in that the encoding relies on four nonorthogonal states based on both quadrature phase amplitudes. Since these states overlap each other, Eve cannot identify them by using any projection operators.

We assume that probe light is a vacuum state, then the solution of the Heisenberg equations of motion in the interaction picture is

\[
\begin{align*}
a_1(t) &= a_1(0) \cos \kappa t, \\
a_2(t) &= a_2(0) \cos \kappa t, \\
p_1(t) &= \sqrt{\omega_s/\omega_p} a_2(0) \sin \kappa t, \\
p_2(t) &= \sqrt{\omega_s/\omega_p} a_1(0) \sin \kappa t.
\end{align*}
\]

The obvious difference from the previous section (6.1) is that the quadrature components for the signal field and the probe field both have to be considered, because the signal is encoded using all possible codings \( a = \{ a_1, -a_1, ia_2, -ia_2 \} \). In the last section, we found that for a vacuum probe field the signal phase is perfectly preserved, except for the attenuation of the light power. The situation in the current system is similar. The difference is that although Eve can extract the signal, there is no any method available for her to detect four nonorthogonal states overlapped each other. We can now conclude that our model is more secure against a QND attack.

In summary, it is possible for us to build a QND apparatus which can extract information from the signal and maintain the signal phase. For Bennett's system, Eve could obtain some information about the key, but the signal sent by
Alice must suffer attenuation subject to the QND measurement. However the information obtained by Eve may not be useful, since Eve is still unable to determine a large fraction of information on the key. In our system based on four nonorthogonal states, Eve can also extract the signal, but it is much harder for her to obtain encoding information. We should point out that even though the QND measurement does not introduce noise and conserves signal phase, quantum measurements on probe states also are subject to the uncertainty principle. This suggests that quantum cryptography is secure against QND attacks.
We have investigated some cryptographic protocols which are based on either the uncertainty principle or Bell's theorem. The focus of these protocols has been on applying quantum principles to computer security in cases unamenable to conventional methods. The protocols we have studied are summarized as follows:

We have presented a quantum cryptographic system based on an optical coupler and modeled by using four nonorthogonal light fields which have been analyzed using quantized quadrature phase amplitudes. This is the first demonstration of the usefulness of quadrature phase amplitudes and the optical coupler to quantum cryptography. Our system has high security against eavesdropping in that the four encoding states are almost indistinguishable – more than 90% superposition, in comparison with the BB protocol which has an inner product value of 0.707 for two nonorthogonal polarized encoding states.

For the case of Bell's theorem, we have undertaken calculations for both photon-based and spin-$\frac{1}{2}$-particle-based systems to study Ekert's protocol. Agreeing with Ekert's result, our calculation demonstrates that eavesdropping leads to no violation of Bell's inequality.

We have investigated quantum conference key protocols. We used information theory to demonstrate the merit of our systems against eavesdropping. The se-
curity in these systems is guaranteed by cryptographic communication in each quantum channel, where any eavesdropping can be detected. Despite some shortcomings on the protocols, our work provides a useful overview on quantum conference key protocols.

We have demonstrated that it is possible for us to build a QND apparatus that can extract some information from the signal in Bennett's two-state system, but it is impossible to obtain sufficient information on the key. Therefore the QND attack fails. On the other hand, we have demonstrated that the QND attack cannot break our system. Our research suggests that all QND schemes encounter a similar difficulty in quantum cryptographic systems. Although it is possible for a QND measurement to maintain signal encoding, we cannot say it is useful since detection on the probe light cannot yield any useful outcome.
REFERENCES


